

拒絶引用S of P 459 WO 03 (X)

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2003年11月20日 (20.11.2003)

PCT

(10) 国際公開番号
WO 03/096608 A1

(51) 国際特許分類⁷: H04L 9/08, 9/14, H04N 11/00, 7/167

(21) 国際出願番号: PCT/JP03/05676

(22) 国際出願日: 2003年5月7日 (07.05.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-135039 2002年5月10日 (10.05.2002) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 伊藤 雄二郎

(ITO, Yujiro) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 下里努 (SHIMOSATO, Tsutomu) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 神原 貞昭 (KAMBARA, Sadaaki); 〒216-0004 神奈川県川崎市宮前区鷺沼3丁目2番6号 鷺沼センタービル 神原特許事務所 Kanagawa (JP).

(81) 指定国 (国内): CN, JP, US.

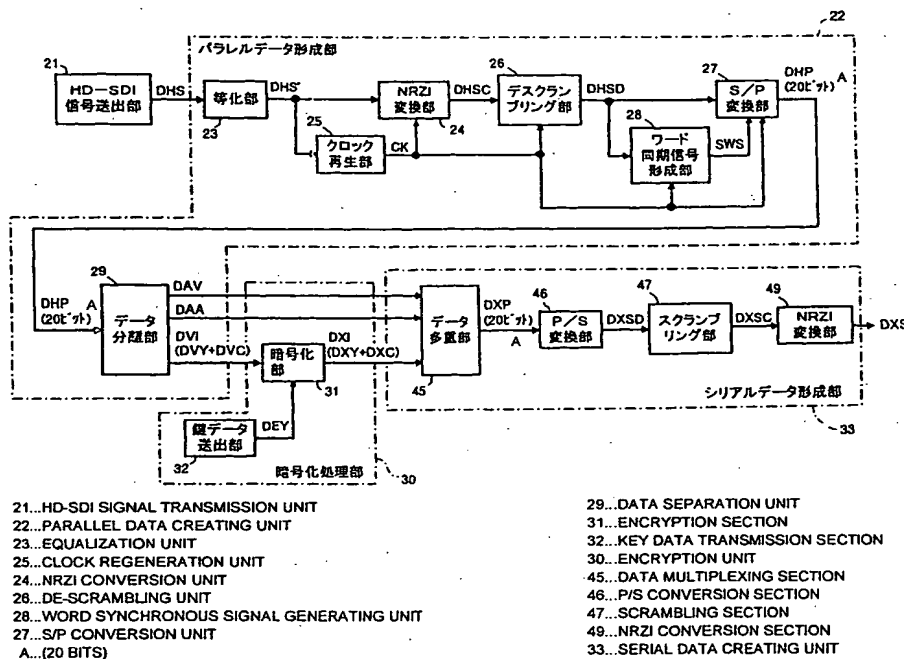
(84) 指定国 (広域): ヨーロッパ特許 (DE, GB).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: DATA TRANSMISSION METHOD AND DATA TRANSMISSION DEVICE

(54) 発明の名称: データ伝送方法及びデータ伝送装置



(57) Abstract: A data transmission method for performing the encryption transmission of digital information data, in which inhibit codes including timing identification codes are set, with no undesired inhibit codes included in the encrypted digital information data. Digital information data in word string data is so encrypted as not to generate any inhibit code. The word string data includes digital information data so created that inhibit codes including a timing identification code are set and timing reference code data

[続葉有]

WO 03/096608 A1



where the timing identification code is used. By the encryption, encrypted digital information data not including any inhibit code is created, and encrypted word string data including the encrypted digital information data and the timing reference code data is created. The encrypted digital information data and the encrypted word string data are sent out for transmission.

(57) 要約: タイミング識別用コードを含む禁止コードが設定されたデジタル情報データについての暗号化伝送を、暗号化されたデジタル情報データを不所望な禁止コードが含まれるものとすることなく行えるデータ伝送方法であって、タイミング識別用コードを含む禁止コードが設定されて形成されたデジタル情報データと、タイミング識別用コードが用いられたタイミング基準コードデータと、を含んだワード列データにおけるデジタル情報データに、禁止コードを発生させない暗号化処理を施して、禁止コードを含まない暗号化されたデジタル情報データを得るとともに、それとタイミング基準コードデータとを含んだ暗号化ワード列データを形成し、それを伝送すべく送出する。

明 細 書

データ伝送方法及びデータ伝送装置

技術分野

本願の請求の範囲に記載された発明は、ディジタル情報データ、もしくは、それにディジタル補助データが付加されて得られる多重データを、それに暗号化処理を施して送出し、送出された暗号化データに復号化処理を施すことにより元のデータを再生できるようにする、データ伝送方法及びその実施に供されるデータ伝送装置に関する。

背景技術

各種の信号情報等をあらわすディジタルデータの伝送にあたり、データ伝送路上での盗聴を防止すべく、送信側において、伝送するディジタルデータを暗号化し、受信側において、暗号化されたディジタルデータについての復号化を行って元のディジタルデータを得るようになることが提案されている。このようなディジタルデータの暗号化にあたっての代表的な暗号アルゴリズムとして、1977年に米国商務省標準局（NBS）が公布したDES（Data Encryption Standard）方式が知られている。

DES方式による暗号化伝送にあっては、ディジタルデータが別途用意される鍵データ（暗号化鍵データ）により定められる規則に従って暗号化されるとともに、暗号化されたディジタルデータが別途用意される鍵データ（復号化鍵データ）により定められる規則に従って復号化され、その際、暗号化鍵データと復号化鍵データとは同じ鍵データ（共通鍵データ）とされる。そして、暗号化及び復号化のためのアルゴリズム自体は公開されており、共通鍵データが秘密に維持されることにより守秘機能が果たされる。

図1は、DES方式による暗号化伝送システムの基本的構成を示す。この図1に示される基本構成にあっては、伝送されるべきディジタルデータが、元データとして、DES暗号化部11に供給される。DES暗号化部11には予め用意された暗号化鍵データも供給され、DES暗号化部11において、元データに暗号化鍵データによって定められる規則に従ったDES方式による暗号化処理が施されて、暗号化データが形成される。そして、DES暗号化部11から暗号化データが送出され、一端がDES暗号化部11に接続されたデータ伝送路12を通じて伝送される。

データ伝送路12を通じて伝送された暗号化データは、データ伝送路12の他端に接続されたDES復号化部13に供給される。DES復号化部13には暗号化鍵データと同一の内容を有するものとされた復号化鍵データも供給され、DES復号化部13において、暗号化データに復号化鍵データによって定められる規則に従ったDES方式による復号化処理が施されて、元データが再生される。

一方、映像信号の分野においては、伝達情報の多様化及び再生画像の高品質化を実現する観点等からのデジタル化が図られており、例えば、映像信号情報をあらわすデジタルデータによって形成されるデジタル映像信号を扱う高精細度テレビジョン (High Definition Television : HDTV) システム等が提案されている。HDTV システムのもとにおけるデジタル映像信号 (以下、HD 信号という) は、例えば、BTA (Broadcasting Technology Association: 放送技術開発協議会) により制定された規格 BTA S-002 に従って形成され、Y, P_B / P_R 形式のものと G, B, R 形式のものがある。Y, P_B / P_R 形式の場合、Y は輝度信号を意味し、 P_B / P_R は色差信号を意味する。また、G, B, R 形式の場合、G, B 及び R は、夫々、緑色原色信号、青色原色信号及び赤色原色信号を意味する。

このような HD 信号は、例えば、各フレーム期間が第 1 フィールド期間と第 2 フィールド期間とに分けられるもとで、フレームレートを 30 Hz (フィールドレートは 60 Hz) とし、各フレーム期間におけるライン数を 1125 ラインとし、ラインあたりのデータサンプル数を 2,200 サンプルとし、サンプリング周波数を 74.25 MHz とするものとされる。そして、例えば、Y, P_B / P_R 形式の HD 信号は、図 2 に示される如くのデータフォーマットに従うものとされる。

図 2 に示されるデータフォーマットにおいて、図 2 の A は、映像信号における輝度信号成分をあらわす輝度信号データ系列 (Y データ系列) における各ライン分の一部を示し、図 2 の B は、映像信号における色差信号成分をあらわす色差信号データ系列 (P_B / P_R データ系列) における各ライン分の一部を示している。Y データ系列及び P_B / P_R データ系列の夫々を形成するワードデータの各々は、例えば、10 ビット構成とされる。即ち、Y データ系列及び P_B / P_R データ系列の夫々は、例えば、10 ビットワードが連なって形成される 10 ビットワード列データであり、ワード伝送レートは、例えば、74.25 Mwp/s とされる。

Y データ系列にあっては、各ライン分がラインランキング部に映像データ部が連なって形成され、各映像データ部の直前に、各々が 10 ビット構成とされる 4 ワード (3FF (Y), 000 (Y), 000 (Y) 及び XYZ (Y); 3FF 及び 000 の夫々は 16 進表示であって、16 進表示であることをあらわす "h" が付されて 3FFh 及び 000h と記され、また、(Y) は Y データ系列中のワードであることをあらわす。) から成るタイミング基準コードデータ (SAV: Start of Active Video) が配されるときともに、各映像データ部の直後に、各々が 10 ビット構成とされる 4 ワード (3FF (Y), 000 (Y), 000 (Y), XYZ (Y)) から成るタイミング基準コードデータ (EAV: End of Active Video) が配される。同様にして、 P_B / P_R データ系列にあっては、各映像データ部の直前に、各々が 10 ビット構成とされる 4 ワード (3FF (C), 000 (C), 000 (C), XYZ (C); (C) は P_B / P_R データ系列中のワードであることをあらわす。) から成る SAV

が配されるとともに、各映像データ部の直後に、各々が10ビット構成とされる4ワード(3FF(C), 000(C), 000(C), XYZ(C))から成るEAVが配される。勿論、Yデータ系列中のEAV及びSAVの夫々は、Yデータ系列における各ラインブランキング部に配され、また、P_B/P_Rデータ系列中のEAV及びSAVの夫々は、P_B/P_Rデータ系列における各ラインブランキング部に配される。

4ワード(3FF(Y), 000(Y), 000(Y), XYZ(Y))もしくは3FF(C), 000(C), 000(C), XYZ(C))については、始めの3ワード(3FF(Y), 000(Y), 000(Y))もしくは3FF(C), 000(C), 000(C))が、ワード同期あるいはライン同期を確立するためのものであり、また、最後の1ワード(XYZ(Y))もしくはXYZ(C))が、同一フレームにおける第1フィールドと第2フィールドとの識別のため、あるいは、タイミング基準コードデータEAVとタイミング基準コードデータSAVとの識別のためのものである。

このようなYデータ系列及びP_B/P_Rデータ系列を含んで構成されるHD信号にあっては、Yデータ系列及びP_B/P_Rデータ系列の夫々について、タイミング基準コードデータSAVもしくはEAVを形成するタイミング識別用コードを含んだ、映像データあるいは補助データ等を形成する情報コードとしては使用されない複数のコードが、禁止コードとして決められている。斯かる禁止コードは、Yデータ系列及びP_B/P_Rデータ系列の夫々が10ビットワード列データであるとき、図3に示される如く、000h~003h及び3FCh~3FFh(16進表現)、即ち、0000000000~0000000011及び1111111100~1111111111とされる。

上述のYデータ系列及びP_B/P_Rデータ系列から成るHD信号が伝送されるに際しては、データ伝送路が簡略化されることからして、ワード列データからシリアルデータに変換されて伝送されるシリアル伝送が望まれることになる。そして、Yデータ系列及びP_B/P_Rデータ系列を含んで形成されるHD信号のシリアル伝送に関しては、前述のBTAによって制定された規格であるBTA S-004によるHD SDI(High Definition Serial Digital Interface)に準拠した伝送を行うことが規格化されている。

HD SDIに準拠した伝送にあっては、Yデータ系列及びP_B/P_Rデータ系列に、各々におけるEAV及びSAVが配されたラインブランキング部が同期せしめられたもとでのワード多重化処理が施されて、図4に示される如くのワード多重データ系列が、ワード伝送レートを $74.25\text{Mwps} \times 2 = 148.5\text{Mwps}$ とする10ビットワード列データとして形成される。このワード多重データ系列にあっては、各映像データ部の直前に、各々が10ビット構成とされる8ワード(3FF(C), 3FF(Y), 000(C), 000(Y), 000(C), 000(Y), XYZ(C), XYZ(Y))から成る多重タイミング基準コードデータ(多重SAV)が

配されるとともに、各映像データ部の直後に、各々が10ビット構成とされる8ワード(3FF(C), 3FF(Y), 000(C), 000(Y), 000(C), 000(Y), XYZ(C), XYZ(Y))から成る多重タイミング基準コードデータ(多重EAV)が配されることになる。

そして、ワード多重データ系列が、それを構成する各10ビットワードについて、最下位ビット(LSB)から最上位ビット(MSB)までが順次送り出されることにより、パラレルデータからシリアルデータに変換され、さらに、そのシリアルデータにスクランブル処理が施されてシリアル伝送HD信号(以下、HD-SDI信号という)とされて、そのHD-SDI信号がデータ伝送路を通じての伝送に供される。斯かるHD-SDI信号は、ビット伝送レートが、例えば、 $148.5 \text{ Mwp s} \times 10 \text{ bit} = 1.485 \text{ Gbps}$ とされる。

上述の如くに、HD-SDI信号がデータ伝送路を通じての伝送に供される際にも、データ伝送路での盗聴を防止すべく、送信側において、HD-SDI信号を暗号化し、受信側において、暗号化されたHD-SDI信号についての復号化を行って元のHD-SDI信号を得るようになることが望まれる場合が考えられる。このような、HD-SDI信号についての暗号化伝送は、原理的には、前述の図1に基本構成が示されるDES方式による暗号化伝送システムと同様な暗号化伝送システムをもって行うことができる。

例えば、HD信号をHD SDIに準拠してHD-SDI信号に変換し、それをデータ伝送路を通じて伝送して、HD-SDI信号をHD SDIに準拠してHD信号に戻し、それに基づく画像表示を行うビデオプロジェクトに供給する場合に、HD-SDI信号についての暗号化伝送を行うとすると、図5に示される如くの暗号化伝送システムが考えられる。

図5に示される暗号化伝送システムにあっては、例えば、ビデオカメラ装置等から得られるHD信号をHD SDIに準拠してHD-SDI信号に変換するHD-SDI信号送出部15から送出されるHD-SDI信号DHSが、HD-SDI暗号化部16に供給される。HD-SDI暗号化部16には、予め用意された暗号化鍵データDDKも供給される。HD-SDI暗号化部16においては、HD-SDI信号DHSが、それにシリアル/パラレル変換(S/P変換)処理が施されて、一旦元のYデータ系列及びP_B/P_Rデータ系列を含んで形成されるHD信号に戻され、そのHD信号における映像データ部に、暗号化鍵データDDKによって定められる規則に従ったDES方式による暗号化処理が施されて、暗号化HD信号が形成され、さらに、暗号化HD信号にパラレル/シリアル変換(P/S変換)処理が施されて暗号化シリアルデータDHSEが形成される。そして、HD-SDI暗号化部16から暗号化シリアルデータDHSEが送出され、一端がHD-SDI暗号化部16に接続されたデータ伝送路17を通じて伝送される。

データ伝送路17を通じて伝送された暗号化シリアルデータDHSEは、データ伝送路17の他端に接続されたHD-SDI復号化部18に供給される。HD-SDI復号化部18には、HD-SDI暗号化部16に供給される暗号化鍵データDDKと同じものである暗号化

鍵データDDKも供給される。HD-SDI復号化部18においては、暗号化シリアルデータDHSEにS/P変換が施されて暗号化HD信号が得られ、その暗号化HD信号における映像データ部に、復号化鍵データDDKによって定められる規則に従ったDES方式による復号化処理が施されて、元のYデータ系列及びP_B/P_Rデータ系列を含んで形成されるHD信号が再生される。さらに、HD-SDI復号化部18においては、再生されたHD信号に、HD-SDIに準拠したYデータ系列及びP_B/P_Rデータ系列の多重化及びそれにより得られるワード多重データ系列に対するP/S変換が行われて元のHD-SDI信号DHSが再生される。

そして、HD-SDI復号化部18から得られるHD-SDI信号DHSが、ビデオプロジェクタ19に供給され、ビデオプロジェクタ19において、HD-SDI信号DHSに基づくHD信号が再生されて、そのHD信号が画像表示に供される。

このようにして、見掛け上は、HD-SDI信号についての暗号化伝送を行うことができることになるが、実際には、上述の図5に示される暗号化伝送システムにあっては、HD-SDI復号化部18における暗号化シリアルデータDHSEについての復号化処理に支障をきたすことになり、さらには、ビデオプロジェクタ19においてHD-SDI信号DHSに基づくHD信号の再生が適正に行えなくなってしまうことになる、重大な問題が生じる。

斯かる問題は、HD-SDI暗号化部16において、HD-SDI信号DHSがHD信号に戻され、そのHD信号の映像データ部に、暗号化鍵データDDKによって定められる規則に従ったDES方式による暗号化処理が施されて、暗号化HD信号が形成されるにあたり、HD信号の映像データ部には禁止コード、即ち、000h~003h及び3FCh~3FFhが含まれていないにもかかわらず、暗号化HD信号の映像データ部には、或る確率をもって、禁止コード、即ち、000h~003h及び3FCh~3FFhが含まれることになってしまい、それにより、映像データ部に禁止コードを含むものとされた暗号化HD信号に基づく暗号化シリアルデータDHSEが形成されて、それがHD-SDI暗号化部16からデータ伝送路17を通じてHD-SDI復号化部18へと伝送されることである。

HD信号において、禁止コードはタイミング基準コードデータSAVもしくはEAVを形成するタイミング識別用コードとして含まれており、HD信号に基づくHD-SDI信号から元のHD信号が再生されるにあたっては、タイミング基準コードデータSAVもしくはEAVを形成する禁止コードがシリアルデータに変換された部分が検出されてワード同期がとられ、その結果、元のHD信号の再生が適正に行われる。ところが、映像データ部に禁止コードを含むものとされた暗号化HD信号に基づく暗号化シリアルデータDHSEが、HD-SDI暗号化部16からデータ伝送路17を通じてHD-SDI復号化部18へと伝送されると、HD-SDI復号化部18において、暗号化シリアルデータDHSEから暗号化HD信号が再生される際に、本来のHD信号に含まれたタイミ

ング基準コードデータSAVもしくはEAVを形成する禁止コードがシリアルデータに変換された部分に加えて、暗号化HD信号における映像データ部に含まれるものとされた禁止コードがシリアルデータに変換された部分も、タイミング基準コードデータSAVもしくはEAVを形成する禁止コードがシリアルデータに変換された部分として検出されてしまう虞が生じる。そして、暗号化HD信号における映像データ部に含まれるものとされた禁止コードがシリアルデータに変換された部分も、タイミング基準コードデータSAVもしくはEAVを形成する禁止コードがシリアルデータに変換された部分として検出されると、暗号化シリアルデータDHSEから暗号化HD信号が再生されるにあたって、正しいワード同期がとられないことになり、暗号化HD信号の再生が適正に行われなくなってしまう。

また、その結果、ビデオプロジェクタ19に供給されるHD-SDI復号化部18からのHD-SDI信号DHSが、適正な内容を有するものとされなくなり、ビデオプロジェクタ19において、HD-SDI復号化部18からのHD-SDI信号DHSに基づいて再生されるHD信号が、適正な映像データ部を有したものとされなくなってしまうのである。

このような不都合は、全て、HD-SDI暗号化部16において、HD-SDI信号DHSがHD信号に戻され、そのHD信号の映像データ部に、暗号化鍵データDDKによって定められる規則に従ったDES方式による暗号化処理が施されることにより暗号化HD信号が形成され、それに基づくシリアルデータDHSEが得られて伝送されるにあたり、暗号化HD信号の映像データ部に、或る確率をもって、禁止コードが含まれることになり、その結果、シリアルデータDHSEが、不所望な禁止コードがシリアルデータに変換された部分を含むことになってしまうことに起因する。

斯かる点に鑑み、本願の請求の範囲に記載された発明は、例えば、HD-SDI信号の如くの、タイミング識別用コードを含む複数のコードが禁止コードとされて形成されたデジタル情報データとタイミング識別用コードが用いられたタイミング基準コードデータとを含んだワード列データに基づくシリアルデータに応じた、デジタル情報データに暗号化処理を施して形成した暗号化シリアルデータを伝送するデータ暗号化伝送に適用されるとき、当該データ暗号化伝送を、暗号化シリアルデータが不所望な禁止コードがシリアルデータに変換された部分を含むものとなる事態を回避できるもとので行えることになるデータ伝送方法、及び、その実施に供されるデータ伝送装置を提供し、さらに、例えば、HD-SDI信号の如くの、タイミング識別用コードを含む複数のコードが禁止コードとされて形成されたデジタル情報データとタイミング識別用コードが用いられたタイミング基準コードデータとを含んだワード列データに基づくシリアルデータについての、それに基づくデジタル情報データに暗号化処理を施して形成した暗号化シリアルデータを伝送するとともに、伝送された暗号化シリアルデータに基づく暗号化処理が施されたデジタル情報データに復号化処理を施して、元のデジタル情報データを得るデータ暗号化伝送に適用されるとき、当該データ暗号

化伝送を、暗号化シリアルデータが、不所望な禁止コードがシリアルデータに変換された部分を含むものとなる事態を回避でき、さらに、伝送された暗号化シリアルデータに基づく暗号化処理が施されたデジタル情報データに復号化処理を施すことにより、元のデジタル情報データを確実に再生できるもとで行えることになるデータ伝送方法、及び、その実施に供されるデータ伝送装置を提供する。

発明の開示

本願の請求の範囲における第1項から第8項までのいずれかに記載された発明に係るデータ伝送方法は、タイミング識別用コードを含む複数のコードが、情報をあらわす情報コードとしては使用されない禁止コードとされて形成されたデジタル情報データと、タイミング識別用コードが用いられたタイミング基準コードデータと、を含んだワード列データにおけるデジタル情報データに、禁止コードを発生させない暗号化処理を施して、禁止コードを含まない暗号化デジタル情報データを得るとともに、その暗号化デジタル情報データとタイミング基準コードデータとを含んだ暗号化ワード列データを形成し、その暗号化ワード列データを伝送すべく送出するものとされる。

本願の請求の範囲における第9項から第16項までのいずれかに記載された発明に係るデータ伝送装置は、タイミング識別用コードを含む複数のコードが、情報をあらわす情報コードとしては使用されない禁止コードとされて形成されたデジタル情報データと、タイミング識別用コードが用いられたタイミング基準コードデータと、を含んだワード列データにおけるデジタル情報データに、禁止コードを発生させない暗号化処理を施して、禁止コードを含まない暗号化デジタル情報データを得る暗号化処理部と、暗号化処理部から得られる暗号化デジタル情報データとタイミング基準コードデータとを含んだ暗号化ワード列データを形成するデータ多重部と、データ多重部から得られる暗号化ワード列データを伝送すべく送出するデータ送出部と、を備えて構成される。

本願の請求の範囲における第17項から第24項までのいずれかに記載された発明に係るデータ伝送方法は、タイミング識別用コードを含む複数のコードが、情報をあらわす情報コードとしては使用されない禁止コードとされて形成されたデジタル情報データと、タイミング識別用コードが用いられたタイミング基準コードデータと、を含んだワード列データにおけるデジタル情報データに、禁止コードを発生させない暗号化処理を施して、禁止コードを含まない暗号化デジタル情報データを得るとともに、その暗号化デジタル情報データとタイミング基準コードデータとを含んだ暗号化ワード列データを形成し、その暗号化ワード列データを伝送すべく送出し、送出された暗号化ワード列データを得て、その暗号化ワード列データから取り出された暗号化デジタル情報データに復号化処理を施して再生デジタル情報データを得る

とともに、その再生デジタル情報データとタイミング基準コードデータとを含んだ再生ワード列データを形成するものとされる。

そして、本願の請求の範囲における第25項から第32項までのいずれかに記載された発明に係るデータ伝送装置は、タイミング識別用コードを含む複数のコードが、情報をあらわす情報コードとしては使用されない禁止コードとされて形成されたデジタル情報データと、タイミング識別用コードが用いられたタイミング基準コードデータと、を含んだワード列データにおけるデジタル情報データに、禁止コードを発生させない暗号化処理を施して、禁止コードを含まない暗号化デジタル情報データを得る暗号化処理部と、暗号化処理部から得られる暗号化デジタル情報データとタイミング基準コードデータとを含んだ暗号化ワード列データを形成する第1のデータ多重部と、第1のデータ多重部から得られる暗号化ワード列データを伝送すべく送出するデータ送出部と、データ送出部により送出された暗号化ワード列データを得て、その暗号化ワード列データから取り出された暗号化デジタル情報データに、復号化処理を施して再生デジタル情報データを得る復号化処理部と、復号化処理部から得られる再生デジタル情報データとタイミング基準コードデータとを含んだ再生ワード列データを形成する第2のデータ多重部と、を備えて構成される。

上述の如くの本願の請求の範囲における第1項から第8項までのいずれかに記載された発明に係るデータ伝送方法、もしくは、本願の請求の範囲における第9項から第16項までのいずれかに記載された発明に係るデータ伝送装置にあっては、デジタル情報データと禁止コードが用いられたタイミング基準コードデータとを含んだワード列データにおけるデジタル情報データに、禁止コードを発生させない暗号化処理が施されて、禁止コードを含まない暗号化デジタル情報データが得られるとともに、その暗号化デジタル情報データとタイミング基準コードデータとを含んだ暗号化ワード列データが形成され、その暗号化ワード列データが伝送されるべく送出される。

このように、禁止コードを含まない暗号化デジタル情報データが形成され、それとタイミング基準コードデータとを含んだ暗号化ワード列データが伝送されるべく送出されるので、送出される暗号化ワード列データに基づく暗号化シリアルデータが形成される場合において、その暗号化シリアルデータが、不所望な禁止コードがシリアルデータに変換された部分を含むものとなる事態はもたらされない。

従って、本願の請求の範囲における第1項から第8項までのいずれかに記載された発明に係るデータ伝送方法、もしくは、本願の請求の範囲における第9項から第16項までのいずれかに記載された発明に係るデータ伝送装置が、例えば、HD-SDI信号の如くの、タイミング識別用コードを含む複数のコードが禁止コードとされて形成されたデジタル情報データとタイミング識別用コードが用いられたタイミング基準コードデータとを含んだワード列データに基づくシリアルデータに応じた、デジタル情報データに暗号化処理を施して形成した暗号化シリアルデータを伝送するデータ暗号

化伝送に適用されるとき、斯かるデータ暗号化伝送が、伝送される暗号化シリアルデータに不所望な禁止コードがシリアルデータに変換された部分が含まれることなく、行われることになる。

また、本願の請求の範囲における第17項から第24項までのいずれかに記載された発明に係るデータ伝送方法、もしくは、本願の請求の範囲における第25項から第32項までのいずれかに記載された発明に係るデータ伝送装置にあっては、デジタル情報データと禁止コードが用いられたタイミング基準コードデータとを含んだワード列データにおけるデジタル情報データに、禁止コードを発生させない暗号化処理が施されて、禁止コードを含まない暗号化デジタル情報データが得られるとともに、その暗号化デジタル情報データとタイミング基準コードデータとを含んだ暗号化ワード列データが形成され、その暗号化ワード列データが伝送されるべく送出され、さらに、送出された暗号化ワード列データから取り出された暗号化デジタル情報データに復号化処理が施されて、再生デジタル情報データが得られ、それとタイミング基準コードデータとを含んだ再生ワード列データが形成される。

このように、禁止コードを含まない暗号化デジタル情報データが形成され、それとタイミング基準コードデータとを含んだ暗号化ワード列データが伝送されるべく送出されるので、送出される暗号化ワード列データに基づく暗号化シリアルデータが形成される場合において、その暗号化シリアルデータが、不所望な禁止コードがシリアルデータに変換された部分を含むものとなる事態はもたらされず、また、伝送された暗号化シリアルデータに基づいて元のシリアルデータが再生される場合において、元のシリアルデータの再生が適正に行われる。そして、送出された暗号化ワード列データから取り出された暗号化デジタル情報データに対する復号化処理を含んだ処理により、送出された暗号化ワード列データに基づく再生ワード列データの形成が確実に行われる。

従って、本願の請求の範囲における第17項から第24項までのいずれかに記載された発明に係るデータ伝送方法、もしくは、本願の請求の範囲における第25項から第32項までのいずれかに記載された発明に係るデータ伝送装置が、例えば、HD-SDI信号の如くの、タイミング識別用コードを含む複数のコードが禁止コードとされて形成されたデジタル情報データとタイミング識別用コードが用いられたタイミング基準コードデータとを含んだワード列データに基づくシリアルデータに応じた、デジタル情報データに暗号化処理を施して形成した暗号化シリアルデータを伝送し、伝送された暗号化シリアルデータに基づいて元のシリアルデータを再生するデータ暗号化伝送に適用されるとき、斯かるデータ暗号化伝送が、伝送される暗号化シリアルデータに不所望な禁止コードがシリアルデータに変換された部分が含まれることなく、かつ、元のシリアルデータが確実に再生されるもとで行われることになる。

図面の簡単な説明

図1は、DES方式による暗号化伝送システムの基本的構成を示すブロック構成図である。

図2のA及びBは、HD信号のデータフォーマットの一例の説明に供される概念図である。

図3は、HD信号についての禁止コードを示す表図である。

図4は、HD信号のデータフォーマットの一例の説明に供される概念図である。

図5は、HD-SDI信号についての暗号化伝送にあたって考えられる暗号化伝送システムの例を示すブロック構成図である。

図6は、本願の請求の範囲における第1項または第2項に記載された発明に係るデータ伝送方法の例が実施される、本願の請求の範囲における第9項または第10項に記載された発明に係るデータ伝送装置の例を示すブロック構成図である。

図7は、図6に示される例における暗号化部31の具体構成例を示すブロック構成図である。

図8は、図7に示されるYデータ暗号化部の第1の具体構成例を示すブロック構成図である。

図9は、図7に示されるCデータ暗号化部の第1の具体構成例を示すブロック構成図である。

図10は、図8に示されるメモリ部及び図9に示されるメモリ部におけるデータの書込み及び読出しの説明に供される概念図である。

図11は、図7に示されるYデータ暗号化部の第2の具体構成例を示すブロック構成図である。

図12は、図7に示されるCデータ暗号化部の第2の具体構成例を示すブロック構成図である。

図13は、図11に示される加減モジュロ演算部及び図12に示される加減モジュロ演算部の動作説明に供される概念図である。

図14は、図7に示されるYデータ暗号化部の第3の具体構成例を示すブロック構成図である。

図15は、図7に示されるCデータ暗号化部の第3の具体構成例を示すブロック構成図である。

図16は、図14に示されるメモリ部及び図15に示されるメモリ部におけるデータの書込み及び読出しの説明に供される概念図である。

図17は、図8、図9、図11、図12、図14及び図15の夫々に示される乱数発生部に代えて用いることができる乱数発生部の他の例を示すブロック構成図である。

図18は、図7に示されるYデータ暗号化部の第4の具体構成例を示すブロック構成図である。

図19は、図7に示されるCデータ暗号化部の第4の具体構成例を示すブロック構成図である。

図20は、図7に示されるYデータ暗号化部の第5の具体構成例を示すブロック構成図である。

図21は、図7に示されるCデータ暗号化部の第5の具体構成例を示すブロック構成図である。

図22は、図18、図19、図20及び21の夫々に示される乱数発生部に代えて用いることができる乱数発生部の他の例を示すブロック構成図である。

図23は、図6との組合せをもって、本願の請求の範囲における第17項または第18項に記載された発明に係るデータ伝送方法の例が実施される、本願の請求の範囲における第25項または第26項に記載された発明に係るデータ伝送装置の例を示すブロック構成図である。

図24は、図23に示される例における復号化部の具体構成例を示すブロック構成図である。

図25は、図24に示されるYデータ復号化部の第1の具体構成例を示すブロック構成図である。

図26は、図24に示されるCデータ復号化部の第1の具体構成例を示すブロック構成図である。

図27は、図24に示されるYデータ復号化部の第2の具体構成例を示すブロック構成図である。

図28は、図24に示されるCデータ復号化部の第2の具体構成例を示すブロック構成図である。

図29は、図24に示されるYデータ復号化部の第3の具体構成例を示すブロック構成図である。

図30は、図24に示されるCデータ復号化部の第3の具体構成例を示すブロック構成図である。

図31は、図25、図26、図27、図28、図29及び図30の夫々に示される乱数発生部に代えて用いることができる乱数発生部の他の例を示すブロック構成図である。

図32は、図24に示されるYデータ復号化部の第4の具体構成例を示すブロック構成図である。

図33は、図24に示されるCデータ復号化部の第4の具体構成例を示すブロック構成図である。

図34は、図24に示されるYデータ復号化部の第5の具体構成例を示すブロック構成図である。

図35は、図24に示されるCデータ復号化部の第5の具体構成例を示すブロック

構成図である。

図 3 6 は、図 3 2, 図 3 3, 図 3 4 及び 3 5 の夫々に示される乱数発生部に代えて用いることができる乱数発生部の他の例を示すブロック構成図である。

発明を実施するための最良の形態

図 6 は、本願の請求の範囲における第 1 項または第 2 項に記載された発明に係るデータ伝送方法の例が実施される、本願の請求の範囲における第 9 項または第 1 0 項に記載された発明に係るデータ伝送装置の例を示す。

図 6 に示される例においては、HD-SDI 信号送出部 2 1 から送出される HD-SDI 信号 D H S がパラレルデータ形成部 2 2 に供給される。HD-SDI 信号 D H S は、例えば、図 2 の A 及び B に示される如くの、各々が、1 0 ビットワード列データとされた Y データ系列と P_B / P_R データ系列とを含んで構成される HD 信号に、HD SDI に準拠した Y データ系列及び P_B / P_R データ系列の多重化及びそれにより得られるワード多重データ系列に対する P / S 変換が行われて形成される。

その際、HD 信号を構成する Y データ系列及び P_B / P_R データ系列の夫々は、タイミング識別コード 3 F F h 及び 0 0 0 h が用いられて形成されたタイミング基準コードデータ S A V 及び E A V を含み、また、各々の映像データ部が、タイミング識別コード 3 F F h 及び 0 0 0 h を含む、図 3 に示される如くの、8 個のコード 0 0 0 h ~ 0 0 3 h 及び 3 F C h ~ 3 F F h を、情報をあらわす情報コードとしては用いられない禁止コードとしたもとで形成されたものとされる。従って、HD-SDI 信号 D H S は、禁止コードに関しては、タイミング基準コードデータ S A V もしくは E A V を形成するタイミング識別コードとされる 3 F F h 及び 0 0 0 h が、3 F F h, 0 0 0 h, 0 0 0 h という順序で配列されてシリアルデータに変換されたものとして含んでいることになる。

パラレルデータ形成部 2 2 にあっては、等化部 2 3 において、HD-SDI 信号 D H S に、それがケーブル伝送により受ける主として高周波数成分の減衰に対処するための適正な等化处理を施し、等化处理が施された HD-SDI 信号 D H S' を形成する。等化部 2 3 から得られる HD-SDI 信号 D H S' は、NR Z I 変換部 2 4 及びクロック再生部 2 5 に供給される。クロック再生部 2 5 にあっては、HD-SDI 信号 D H S' についてのクロック信号 C K を再生する。

クロック再生部 2 5 から得られるクロック信号 C K は、NR Z I 変換部 2 4 に供給され、NR Z I 変換部 2 4 は、HD-SDI 信号 D H S' についてのクロック信号 C K を用いての NR Z I (Nonreturn to Zero Inverted) 変換を行う。それにより、NR Z I 変換部 2 4 から NR Z I 変換がなされた HD-SDI 信号 D H S C が送出されて、それがデスクランプリング部 2 6 に供給される。デスクランプリング部 2 6 には、クロック再生部 2 5 から得られるクロック信号 C K も供給され、デスクランプリング部 2 6 は、HD

-SDI信号DHSCにかけられたスクランブル処理を解除する。そして、デスクランプリング部26からスクランブル処理が解除されたHD-SDI信号DHSDが導出されて、それがS/P変換部27及びワード同期信号形成部28に供給される。

ワード同期信号形成部28にあつては、クロック再生部25から得られるクロック信号CKも供給され、斯かるもとにおいて、HD-SDI信号DHSDに含まれる、タイミング基準コードデータSAVもしくはEAVを形成するタイミング識別コードとされる3FFh及び000hが、3FFh, 000h, 000hという順序で配列されてシリアルデータに変換された部分についての検出を行い、斯かる部分を検出したとき、ワード同期信号SWSを送出する。ワード同期信号形成部28から送出されるワード同期信号SWSは、S/P変換部27に供給される。S/P変換部27にあつては、クロック再生部25から得られるクロック信号CKも供給され、斯かるもとにおいて、HD-SDI信号DHSDに対する、ワード同期信号SWSに従ったワード同期がとられたもとでのS/P変換処理を行う。このようなS/P変換処理により、HD-SDI信号DHSDを、各々が10ビットワード列データとされたYデータ系列とP_B/P_Rデータ系列とが、タイミング基準コードデータSAV及びEAVについての同期がとられたもとでビット重畳されて得られるものとされる、20ビットワード列データDHPに変換する。

S/P変換部27から得られる20ビットワード列データDHPは、データ分離部29に供給される。データ分離部29にあつては、20ビットワード列データDHPを、重畳タイミングデータDAV, 重畳補助データDAA及び重畳映像データDVIに分割する。重畳タイミングデータDAVは、10ビットワード列を成すYデータ系列におけるタイミング基準コードデータEAV及びSAV, ライン番号データ, 誤り検出符号データ等と、10ビットワード列を成すP_B/P_Rデータ系列におけるタイミング基準コードデータEAV及びSAV, ライン番号データ, 誤り検出符号データ等とが、ワード同期がとられたもとでビット重畳されて得られる20ビットワード列データとされる。また、重畳補助データDAAは、10ビットワード列を成すYデータ系列における補助データと10ビットワード列を成すP_B/P_Rデータ系列における補助データとが、ワード同期がとられたもとでビット重畳されて得られる20ビットワード列データとされる。さらに、重畳映像データDVIは、10ビットワード列を成すYデータ系列における映像データ部を構成するY信号映像データD.VYと10ビットワード列を成すP_B/P_Rデータ系列における映像データ部を構成するC信号映像データD.VCとが、ワード同期がとられたもとでビット重畳されて得られる20ビットワード列データとされる。

データ分離部29から得られる重畳タイミングデータDAV, 重畳補助データDAA及び重畳映像データDVIは、パラレルデータ形成部22から送出されて、暗号化処理部30に供給される。暗号化処理部30は、暗号化部31と鍵データ送出部32

とを含んで構成されている。

データ分離部29からの重畳タイミングデータDAV及び重畳補助データDAAは、暗号化処理部30を素通りするものとされて、シリアルデータ形成部33に供給される。一方、データ分離部29からの重畳映像データDVIは、暗号化部31に供給される。鍵データ送出部32は、予め設定された鍵データDEYを暗号化部31に供給する。

暗号化部31は、20ビットワード列データである重畳映像データDVIに対して、鍵データDEYにより定められる規則に従った、例えば、DES方式、あるいは、他の方式による暗号化処理を施し、重畳映像データDVIに基づく暗号化映像データDXIを、20ビットワード列データを成すものとして形成する。

図7は、暗号化部31の具体構成例を示す。この図7に示される暗号化部31の具体構成例にあつては、20ビットワード列データである重畳映像データDVIがビット分割部40に供給される。ビット分割部40は、重畳映像データDVIを、10ビットワード列を成すY信号映像データDVYと10ビットワード列を成すC信号映像データDVCとに分割し、それらを個別に導出する。

ビット分割部40から得られるY信号映像データDVY及びC信号映像データDVCは、Yデータ暗号化部41及びCデータ暗号化部42に夫々供給される。Yデータ暗号化部41及びCデータ暗号化部42の夫々には、鍵データ送出部32からの鍵データDEYも供給される。

Yデータ暗号化部41は、10ビットワード列を成すY信号映像データDVYに、鍵データDEYにより定められる規則に従ったDES方式による暗号化処理を施し、Y信号映像データDVYに基づく暗号化Y信号映像データDXYを10ビットワード列を成すものとして形成する。また、Cデータ暗号化部42は、10ビットワード列を成すC信号映像データDVCに、鍵データDEYにより定められる規則に従ったDES方式による暗号化処理を施し、C信号映像データDVCに基づく暗号化C信号映像データDXCを10ビットワード列データを成すものとして形成する。

斯かる際、Yデータ暗号化部41にあつては、Y信号映像データDVYに対する暗号化処理を、禁止コード000h～003h及び3FCh～3FFhを発生させないようにして行い、Y信号映像データDVYに基づく暗号化Y信号映像データDXYを、禁止コード000h～003h及び3FCh～3FFhを含まない10ビットワード列データとなす。同様に、Cデータ暗号化部42にあつては、C信号映像データDVCに対する暗号化処理を、禁止コード000h～003h及び3FCh～3FFhを発生させないようにして行い、C信号映像データDVCに基づく暗号化C信号映像データDXCを、禁止コード000h～003h及び3FCh～3FFhを含まない10ビットワード列データとなす。

このようにして、Yデータ暗号化部41及びCデータ暗号化部42から夫々得られ

る、10ビットワード列データを成す暗号化Y信号映像データDX Y及び10ビットワード列データを成す暗号化C信号映像データDX Cは、ビット重畳部43に供給される。そして、ビット重畳部43にあっては、10ビットワード列データを成す暗号化Y信号映像データDX Yと10ビットワード列データを成す暗号化C信号映像データDX Cとを重畳して、20ビットワード列データを成す暗号化映像データDX Iを形成し、それを暗号化部31の出力データとして送出する。この20ビットワード列データを成す暗号化映像データDX Iも、禁止コード000h~003h及び3FCh~3FFhを含まないものとされることになる。

暗号化部31の出力データとされる暗号化映像データDX Iは、暗号化処理部30から送出されて、シリアルデータ形成部33に供給される。シリアルデータ形成部33にあっては、データ分離部29から送出されて暗号化処理部30を素通りした、各々が20ビットワード列データを成す重畳タイミングデータDA V及び重畳補助データDAAと、暗号化処理部30から送出された20ビットワード列データを成す暗号化映像データDX Iとが、データ多重部45に供給される。

データ多重部45にあっては、暗号化映像データDX I、重畳タイミングデータDA V及び重畳補助データDAAに多重化処理を施して、暗号化映像データDX Iと重畳タイミングデータDA Vと重畳補助データDAAとを含んで成る暗号化20ビットワード列データDX Pを形成する。このようにして、データ多重部45において得られる暗号化20ビットワード列データDX Pは、P/S変換部46に供給される。

P/S変換部46にあっては、暗号化20ビットワード列データDX PにP/S変換処理を施して、暗号化20ビットワード列データDX Pに基づく暗号化シリアルデータDX S Dを形成し、それをスクランプリング部47に供給する。

スクランプリング部47は、暗号化シリアルデータDX S Dにスクランブル処理を施し、スクランブル処理がかけられた暗号化シリアルデータDX S Cを形成して、それをNRZ I変換部49に供給する。NRZ I変換部49は、スクランブル処理がかけられた暗号化シリアルデータDX S CについてのNRZ I変換を行う。それにより、NRZ I変換部49において、暗号化されたHD-SDI信号、即ち、暗号化HD-SDI信号DX Sが形成され、それがシリアルデータ形成部33から、例えば、同軸ケーブルを通じて伝送されるべく送出される。

斯かるもとにおいて、シリアルデータ形成部33は、それに含まれるデータ多重部45以外の部分が、データ多重部45において得られる暗号化20ビットワード列データDX Pを伝送すべく送出するデータ送出部を形成していることになる。

図8及び図9は、夫々、図7に示されるYデータ暗号化部41及びCデータ暗号化部42についての第1の具体構成例を示す。図8に示される第1の具体構成例が採用されたYデータ暗号化部41及び図9に示される第1の具体構成例が採用されたCデータ暗号化部42が用いられて、図6に示される暗号化部31が構成される場合には、

その際に図6があらわす構成は、本願の請求の範囲における第3項、第4項、第5項または第6項に記載された発明に係るデータ伝送方法の例が実施される、本願の請求の範囲における第11項、第12項、第13項または第14項に記載された発明に係るデータ伝送装置の例を示すことになる。

図8に示されるYデータ暗号化部41についての第1の具体構成例は、10ビットワード列データを成すY信号映像データDVYが第1の読出アドレスデータとして供給されるメモリ部51と、鍵データDEYが供給される乱数発生部52と、を備えて構成されている。

乱数発生部52にあっては、レジスタ部53が、入力データに応答して、例えば、128ビット構成とされるレジスタ出力データDRZを送出し、それをDES暗号形成部54に供給する。このレジスタ部53には、初期入力データDITが供給される。

DES暗号形成部54には、鍵データDEYも供給され、DES暗号形成部54は、レジスタ出力データDRZについての鍵データDEYによって定められる規則に従ったDES方式の暗号化を行い、例えば、128ビット構成とされる暗号データDEZを送出する。DES暗号形成部54から得られる暗号データDEZは、ビット取出部55に供給されるとともに、レジスタ部53に入力データとして帰還される。それゆえ、レジスタ部53は、最初に、初期入力データDITに応じたレジスタ出力データDRZを送出し、その後は、DES暗号形成部54から得られる暗号データDEZに応じたレジスタ出力データDRZを送出することになる。

ビット取出部55は、DES暗号形成部54から得られる暗号データDEZを形成する128ビットのうちの10ビットを、擬似乱数データDXAとして取り出す。ビット取出部55から得られる擬似乱数データDXAは、乱数発生部52から送出されて、メモリ部51に第2の読出アドレスデータとして供給される。

メモリ部51にあっては、禁止コード000h~003h及び3FCh~3FFhが除かれた10ビットコードを有した1024-8=1016個の10ビットワードデータが格納されている。これらの1016個の10ビットワードデータは、夫々が有する10ビットコードが、メモリ部51に第1の読出アドレスデータとして供給されるY信号映像データDVYを形成する10ビットワードの夫々が有する10ビットコードと、1対1の特定の対応関係を取り、その特定の対応関係のもとに、Y信号映像データDVYに応じてメモリ部51から読み出されるとともに、斯かる特定の対応関係が、メモリ部51に第2の読出アドレスデータとして供給される擬似乱数データDXAに応じて変化するものとされる。

例えば、Y信号映像データDVYを形成する10ビットワードが夫々有する10ビットコードを映像ワードデータコードと呼び、メモリ部51に格納された1016個の10ビットワードデータが夫々有する10ビットコードを格納ワードデータコードと呼ぶと、擬似乱数データDXAが或る状態をとるとき、映像ワードデータコードと

格納ワードデータコードとは、例えば、図10において矢印が付された線で示される如くの1対1の対応関係を取り、斯かる対応関係のもとに、各映像ワードデータコードを有した10ビットワードに応じて、各格納ワードデータコードを有する10ビットワードデータが、矢印が付された線に従って読み出される。そして、擬似乱数データDXAが変化すると、それに応じて、矢印が付された線で示される映像ワードデータコードと格納ワードデータコードとの1対1の対応関係が変化せしめられる。

上述の如くにしてメモリ部51から読み出される格納ワードデータコードを有した10ビットワードデータは、順次配列されて、10ビットワード列データを成す暗号化Y信号映像データDXYを形成する。従って、Y信号映像データDXYは、メモリ部51において、擬似乱数データDXAに応じた禁止コードを含まないコードへのコード変換を受けて、暗号化Y信号映像データDXYに変換されることになる。その結果、暗号化Y信号映像データDXYは、禁止コードを含まないものとされる。

図9に示されるCデータ暗号化部42についての第1の具体構成例は、10ビットワード列データを成すC信号映像データDVCが第1の読出アドレスデータとして供給されるメモリ部56と、鍵データDEYが供給される乱数発生部57と、を備えて構成されている。

乱数発生部57は、図8に示される乱数発生部52と同様のものであり、それを構成する各部に、図8に示される乱数発生部52における対応する部分と共通の符号を付して示し、重複説明は省略する。この乱数発生部57から送出される擬似乱数データDXAが、メモリ部56に第2の読出アドレスデータとして供給される。

メモリ部56にも、禁止コード000h~003h及び3FCh~3FFhが除かれた10ビットコードを有した $1024 - 8 = 1016$ 個の10ビットワードデータが格納されている。そして、これらの1016個の10ビットワードデータは、夫々が有する10ビットコードが、メモリ部56に第1の読出アドレスデータとして供給されるC信号映像データDVCを形成する10ビットワードの夫々が有する10ビットコードと、1対1の特定の対応関係を取り、その特定の対応関係のもとに、C信号映像データDVCに応じてメモリ部56から読み出されるとともに、斯かる特定の対応関係が、メモリ部56に第2の読出アドレスデータとして供給される擬似乱数データDXAに応じて変化するものとされる。

例えば、C信号映像データDVCを形成する10ビットワードが夫々有する10ビットコードを映像ワードデータコードと呼び、メモリ部56に格納された1016個の10ビットワードデータが夫々有する10ビットコードを格納ワードデータコードと呼ぶと、擬似乱数データDXAが或る状態をとるとき、映像ワードデータコードと格納ワードデータコードとは、例えば、図10において矢印が付された線で示される如くの1対1の対応関係を取り、斯かる対応関係のもとに、各映像ワードデータコードを有した10ビットワードに応じて、各格納ワードデータコードを有する10ビット

トワードデータが、矢印が付された線に従って読み出される。そして、擬似乱数データD X Aが変化すると、それに応じて、矢印が付された線で示される映像ワードデータコードと格納ワードデータコードとの1対1の対応関係が変化せしめられる。

上述の如くにしてメモリ部56から読み出される格納ワードデータコードを有した10ビットワードデータは、順次配列されて、10ビットワード列データを成す暗号化C信号映像データD X Cを形成する。従って、C信号映像データD V Cは、メモリ部56において、擬似乱数データD X Aに応じた禁止コードを含まないコードへのコード変換を受けて、暗号化C信号映像データD X Cに変換されることになる。その結果、暗号化C信号映像データD X Cは、禁止コードを含まないものとされる。

上述の図8及び図9に示される具体構成例にあつては、メモリ部51及び56に夫々連結された乱数発生部52及び57が、擬似乱数データD X Aを発生してそれをメモリ部51及び56に供給するものとされているが、乱数発生部52及び57を、擬似乱数データD X Aに代えて、所定の乱数データを発生してそれをメモリ部51及び56に供給するものとなすこともできる。

図11及び図12は、夫々、図7に示されるYデータ暗号化部41及びCデータ暗号化部42についての第2の具体構成例を示す。図11に示される第2の具体構成例が採用されたYデータ暗号化部41及び図12に示される第2の具体構成例が採用されたCデータ暗号化部42が用いられて、図6に示される暗号化部31が構成される場合には、その際に図6があらわす構成は、本願の請求の範囲における第3項、第4項、第5項または第7項に記載された発明に係るデータ伝送方法の第1の例が実施される、本願の請求の範囲における第11項、第12項、第13項または第15項に記載された発明に係るデータ伝送装置の第1の例を示すことになる。

図11に示されるYデータ暗号化部41についての第2の具体構成例は、10ビットワード列データを成すY信号映像データD V Yが供給される加減モジュロ演算部61と、鍵データD E Yが供給される乱数発生部62と、を備えて構成されている。

乱数発生部62は、図8に示される乱数発生部52と同様のものであり、それを構成する各部に、図8に示される乱数発生部52における対応する部分と共通の符号を付して示し、重複説明は省略する。この乱数発生部62から送出される擬似乱数データD X Aは、加減モジュロ演算部61に供給される。

加減モジュロ演算部61にあつては、Y信号映像データD V Yが10ビットワード列データを成し、情報コードが禁止コード000h~003h及び3FCh~3FFhを含まないというだけでなく、禁止コードの範囲が情報コードの範囲外にそれに接して配されていることになるものであることを利用して、Y信号映像データD V Yに対して、擬似乱数データD X Aに応じた、禁止コードを含まないコードへのコード変換を施すための演算（これを、加減モジュロ演算と呼ぶ）を行い、加減モジュロ演算の結果に基づいて定められる変換されたコードを暗号化Y信号映像データD X Yにつ

いてのコードとする。それにより、Y信号映像データDVYが、禁止コードを含まない暗号化Y信号映像データDXYに変換されることになる。

ここでは、Y信号映像データDVYが10ビットワード列データを成すものとされているので、10ビットコードについて考えると、10ビットコードは、000hから3FFhまで、1024個ある。そこで、これらの1024個のコードに、000hから3FFhまで順番に1から1024までのコード位置番号を付すこととする。上述の加減モジュロ演算は、このようなコード位置番号が設定されたもとにおいて、暗号化Y信号映像データDXYを形成する10ビットワードがとるべき10ビットコードのコード位置番号を定めるものとされる。

加減モジュロ演算における演算式は、具体的には、Y信号映像データDVYがとる情報コードのコード位置番号を M_i 、暗号化Y信号映像データDXYがとるべき情報コードのコード位置番号を C_i 、擬似乱数データDXAがとる10ビットコードのコード位置番号を E_i とし、さらに、Y信号映像データDVYがとり得る情報コードの範囲の一端側に配される禁止コードの個数を N_1 、Y信号映像データDVYがとり得る情報コードの個数を N_2 として、下記の〔数1〕によりあらわすことができる。

〔数1〕

$$C_i = \{ (M_i - N_1) + E_i \} \bmod N_2 + N_1$$

但し、 $\{ (M_i - N_1) + E_i \} \bmod N_2$ は、 $\{ (M_i - N_1) + E_i \}$ を N_2 で除した余りを意味する。

Y信号映像データDVYは10ビットワード列データを成すものであるので、 N_1 は、禁止コード000h～003hの個数であり、従って、4となり、また、 N_2 は、10ビットコードの総個数から禁止コードの個数を減じた個数、即ち、 $1024 - 8 = 1016$ となる。

〔数1〕によりあらわされる演算式においては、 M_i から N_1 を減じる減算が行われて、それにより、図13に示される如くに、0004hのコード位置番号5からの3FBhのコード位置番号1020までのコード位置範囲にある、Y信号映像データDVYがとる情報コードのコード位置番号が、000hのコード位置番号1から3F7hのコード位置番号1016までの、有効コードとして扱われる000hから3F7hまでに対応するコード位置番号範囲内のコード位置番号に変換される。続いて、斯かる変換により得られるコード位置番号に、擬似乱数データDXAがとる10ビットコードのコード位置番号が加えられた後、それを1016で除した余りが求められるモジュロ演算が行われる。そして、求められた余りに4を加える加算が行われ、004hのコード位置番号5からの3FBhのコード位置番号1020までのコード位置範囲内のコード位置番号が得られ、それが暗号化Y信号映像データDXYがとるべき情報コードのコード位置番号 C_i とされる。

そして、加減モジュロ演算部61にあっては、このようにして加減モジュロ演算の

結果得られるコード位置番号C_iに対応する10ビットコードが、暗号化Y信号映像データDXYがとる情報コードとされる。斯かる暗号化Y信号映像データDXYがとる情報コードは、Y信号映像データD_VYがとる情報コードが、擬似乱数データDXAがとる10ビットコードに応じた、禁止コードを含まないコードに変換されることにより得られるものである。従って、この情報コードをとる暗号化Y信号映像データDXYは、禁止コードを含まないものとされることになる。

図12に示されるCデータ暗号化部42についての第2の具体構成例は、10ビットワード列データを成すC信号映像データDVCが供給される加減モジュロ演算部63と、鍵データDEYが供給される乱数発生部64と、を備えて構成されている。

乱数発生部64は、図11に示される乱数発生部62と同様のものであり、それを構成する各部に、図11に示される乱数発生部62における対応する部分と共通の符号を付して示し、重複説明は省略する。この乱数発生部64から送出される擬似乱数データDXAは、加減モジュロ演算部63に供給される。

加減モジュロ演算部63にあっては、C信号映像データDVCが10ビットワード列データを成し、情報コードが禁止コード000h~003h及び3FCh~3FFhを含まないというだけでなく、禁止コードの範囲が情報コードの範囲外にそれに接して配されていることになるものであることを利用して、C信号映像データDVCに対して、擬似乱数データDXAに応じた、禁止コードを含まないコードへのコード変換を施すための加減モジュロ演算を行う。このC信号映像データDVCに対する加減モジュロ演算は、上述の図11に示される加減モジュロ演算部61によって行われるY信号映像データD_VYに対しての加減モジュロ演算と同様にして行われ、その結果に基づいて定められる変換されたコードが、暗号化C信号映像データDXCがとる情報コードとされる。斯かる暗号化C信号映像データDXCがとる情報コードは、C信号映像データDVCがとる情報コードが、擬似乱数データDXAがとる10ビットコードに応じた、禁止コードを含まないコードに変換されることにより得られるものである。従って、この情報コードをとる暗号化C信号映像データDXCは、禁止コードを含まないものとされることになる。

上述の図11及び図12に示される具体構成例にあっては、加減モジュロ演算部61及び63に夫々連結された乱数発生部62及び64が、擬似乱数データDXAを発生してそれを加減モジュロ演算部61及び63に供給するものとされているが、乱数発生部62及び64を、擬似乱数データDXAに代えて、所定の乱数データを発生してそれを加減モジュロ演算部61及び63に供給するものとなすこともできる。

図14及び図15は、夫々、図7に示されるYデータ暗号化部41及びCデータ暗号化部42についての第3の具体構成例を示す。図14に示される第3の具体構成例が採用されたYデータ暗号化部41及び図15に示される第3の具体構成例が採用されたCデータ暗号化部42が用いられて、図6に示される暗号化部31が構成される

場合には、その際に図6があらわす構成は、本願の請求の範囲における第3項、第4項、第5項または第8項に記載された発明に係るデータ伝送方法の例が実施される、本願の請求の範囲における第11項、第12項、第13項または第16項に記載された発明に係るデータ伝送装置の例を示すことになる。

図14に示されるYデータ暗号化部41についての第3の具体構成例は、Y信号映像データDVYが、上述の如くに、禁止コードを情報コードの範囲外に配される000h~003h及び3FCh~3FFhとするもとで形成されたものでなく、情報コードと禁止コードとが混在する状態のもとで、情報コードのみが用いられて形成されたものとされる場合に用いられる。そして、図14に示されるYデータ暗号化部41についての第3の具体構成例は、上述の図11に示されるYデータ暗号化部41についての第2の具体構成例に、加減モジュロ演算部61の入力側に配されるメモリ部66が追加されたものに該当するものとして構成される。

メモリ部66には、10ビットワード列データを成すY信号映像データDVYが供給されるが、このY信号映像データDVYは、禁止コードを情報コードの範囲外に配される000h~003h及び3FCh~3FFhとするもとで形成されたものでなく、情報コードと禁止コードとが混在する状態のもとで、情報コードのみが用いられて形成されたものとされる。

メモリ部66においては、Y信号映像データDVYの書込みと読出しとが行われ、メモリ部66から、Y信号映像データDVYに基づく読出Y信号映像データDVYMが送出される。その際、Y信号映像データDVYの書込みにあたっては、Y信号映像データDVYを形成する各10ビットワードが、それがとる10ビットコードに応じて定められた書込アドレスをもって書き込まれ、また、Y信号映像データDVYの読出しにあたっては、Y信号映像データDVYを形成する各10ビットワードが、書込アドレスと1対1の特定の対応関係を有するものとされた読出アドレスをもって読み出される。そして、このような書込アドレスと読出アドレスとの間の1対1の特定の対応関係は、例えば、図16において矢印が付された線で示される如くに、禁止コードに割り当てられる書込アドレスが、情報コードに割り当てられる読出アドレスの範囲外とされる一連の読出アドレスに対応するものとなるようにされる。

それにより、メモリ部66に書き込まれたY信号映像データDVYが読み出されることによりメモリ部66から送出される読出Y信号映像データDVYMが、禁止コードの範囲が情報コードの範囲外にそれに接して配されるもとで形成されたものとされる。即ち、メモリ部66は、情報コードと禁止コードとが混在する状態のもとで、情報コードのみが用いられて形成されたY信号映像データDVYを、禁止コードの範囲が情報コードの範囲外にそれに接して配されるもとで形成されたものとされる読出Y信号映像データDVYMに変換する役割を果たすのである。

メモリ部66から送出される読出Y信号映像データDVYMは、上述の図11に示

2 2

されるYデータ暗号化部41についての第2の具体構成例における加減モジュロ演算部61に供給される、禁止コードが情報コードの範囲外に配される000h~003h及び3FCh~3FFとされているY信号映像データDVYと同様に、禁止コードの範囲が情報コードの範囲外にそれに接して配されていることになる。そして、メモリ部66から送出される読出Y信号映像データDVYMは、加減モジュロ演算部61に供給される。

加減モジュロ演算部61にあっては、読出Y信号映像データDVYMについての加減モジュロ演算を行い、その結果に従って形成される暗号化Y信号映像データDXYを送出する。その際、加減モジュロ演算部61は、読出Y信号映像データDVYMについての加減モジュロ演算を、上述された図11に示される加減モジュロ演算部61によるY信号映像データDVYについての加減モジュロ演算と同様にして行い、その結果に基づいて定められる変換されたコードを、暗号化Y信号映像データDXYについての情報コードとする。それにより、読出Y信号映像データDVYMが、禁止コードを含まない暗号化Y信号映像データDXYに変換されることになる。

このようにして、図14に示されるYデータ暗号化部41についての第3の具体構成例にあっては、Y信号映像データDVYがメモリ部66によって読出Y信号映像データDVYMに変換され、さらに、加減モジュロ演算部61によって読出Y信号映像データDVYMについての変換が行われて、暗号化Y信号映像データDXYが得られる。

図15に示されるCデータ暗号化部42についての第3の具体構成例は、C信号映像データDVCが、禁止コードを情報コードの範囲外に配される000h~003h及び3FCh~3FFhとするもとで形成されたものでなく、情報コードと禁止コードとが混在する状態のもとで、情報コードのみが用いられて形成されたものとされる場合に用いられる。そして、図15に示されるCデータ暗号化部42についての第3の具体構成例は、上述の図12に示されるCデータ暗号化部42についての第2の具体構成例に、加減モジュロ演算部63の入力側に配されるメモリ部67が追加されたものに該当するものとして構成される。

メモリ部67には、10ビットワード列データを成すC信号映像データDVCが供給されるが、このC信号映像データDVCは、禁止コードを情報コードの範囲外に配される000h~003h及び3FCh~3FFhとするもとで形成されたものでなく、情報コードと禁止コードとが混在する状態のもとで、情報コードのみが用いられて形成されたものとされる。

メモリ部67においては、C信号映像データDVCの書込みと読出しとが行われ、メモリ部67から、C信号映像データDVCに基づく読出C信号映像データDVCMが送出される。斯かるメモリ部67におけるC信号映像データDVCの書込み及び読出しは、図14に示されるメモリ部66におけるY信号映像データDVYの書込み及

23

び読出しと同様にして行われ、それにより、メモリ部67から、読出C信号映像データDVCMが、禁止コードの範囲が情報コードの範囲外にそれに接して配されるもとで形成されたものとして送出される。即ち、メモリ部67は、情報コードと禁止コードとが混在する状態のもとで、情報コードのみが用いられて形成されたC信号映像データDVCを、禁止コードの範囲が情報コードの範囲外にそれに接して配されるもとで形成されたものとされる読出C信号映像データDVCMに変換する役割を果たすのである。

メモリ部67から送出される読出C信号映像データDVCMは、上述の図12に示されるCデータ暗号化部42についての第2の具体構成例における加減モジュロ演算部63に供給される、禁止コードが情報コードの範囲外に配される000h~003h及び3FCh~3FFとされているC信号映像データDVCと同様に、禁止コードの範囲が情報コードの範囲外にそれに接して配されていることになる。そして、メモリ部67から送出される読出C信号映像データDVCMは、映加減モジュロ演算部63に供給される。

加減モジュロ演算部63にあっては、読出C信号映像データDVCMについての加減モジュロ演算を行い、その結果に従って形成される暗号化C信号映像データDXCを送出する。その際、加減モジュロ演算部63は、読出C信号映像データDVCMについての加減モジュロ演算を、上述された図12に示される加減モジュロ演算部63によるC信号映像データDVCについての加減モジュロ演算と同様にして行い、その結果に基づいて定められる変換されたコードを、暗号化C信号映像データDXCについての情報コードとする。それにより、読出C信号映像データDVCMが、禁止コードを含まない暗号化C信号映像データDXCに変換されることになる。

このようにして、図15に示されるCデータ暗号化部42についての第3の具体構成例にあっては、C信号映像データDVCがメモリ部67によって読出C信号映像データDVCMに変換され、さらに、加減モジュロ演算部63によって読出C信号映像データDVCMについての変換が行われて、暗号化C信号映像データDXCが得られる。

上述の図14及び図15に示される具体構成例にあっては、加減モジュロ演算部61及び63に夫々連結された乱数発生部62及び64が、擬似乱数データDXAを発生してそれを加減モジュロ演算部61及び63に供給するものとされているが、乱数発生部62及び64を、擬似乱数データDXAに代えて、所定の乱数データを発生してそれを加減モジュロ演算部61及び63に供給するものとなすこともできる。

図17は、図8に示されるYデータ暗号化部41の第1の具体構成例における乱数発生部52、図9に示されるCデータ暗号化部42の第1の具体構成例における乱数発生部57、図11及び図14に夫々示されるYデータ暗号化部41の第2及び第3の具体構成例の各々における乱数発生部62、及び、図12及び図15に夫々示され

るCデータ暗号化部42の第2及び第3の具体構成例の各々における乱数発生部64の夫々に代えて用いることができる乱数発生部の他の例を示す。

この図17に示される乱数発生部52'にあっては、カウンタ部53'が、初期入力データDITに基づく動作を行って、例えば、128ビット構成とされるカウンタ出力データDRZ'を送出し、それをAES暗号形成部54'に供給する。

AES暗号形成部54'は、2001年に米国商務省管轄下の国立標準及び技術研究所(NIST)が公布したAES(Advances Encryption Standard)方式に準拠した暗号化処理を行って、暗号データを形成する。そして、AES暗号形成部54'には、鍵データDEYも供給され、AES暗号形成部54'は、カウンタ出力データDRZ'についての鍵データDEYによって定められる規則に従ったAES方式の暗号化を行い、例えば、128ビット構成とされる暗号データDEZ'を送出する。

AES暗号形成部54'から得られる暗号データDEZ'は、ビット取出部55'に供給され、ビット取出部55'は、暗号データDEZ'を形成する128ビットのうちの10ビットを、擬似乱数データDXA'として取り出す。ビット取出部55'から得られる擬似乱数データDXA'は、乱数発生部52'から送出され、図8に示される乱数発生部52、図9に示される乱数発生部57、図11及び図14の夫々に示される乱数発生部62、及び、図12及び図15の夫々に示される乱数発生部64の各々から送出される擬似乱数データDXAに代わるものとされる。

図18及び図19は、夫々、図7に示されるYデータ暗号化部41及びCデータ暗号化部42についての第4の具体構成例を示す。図18に示される第4の具体構成例が採用されたYデータ暗号化部41及び図19に示される第4の具体構成例が採用されたCデータ暗号化部42が用いられて、図6に示される暗号化部31が構成される場合には、その際に図6があらわす構成は、本願の請求の範囲における第3項、第4項、第5項または第7項に記載された発明に係るデータ伝送方法の第2の例が実施される、本願の請求の範囲における第11項、第12項、第13項または第15項に記載された発明に係るデータ伝送装置の第2の例を示すことになる。

図18に示されるYデータ暗号化部41についての第4の具体構成例は、10ビットワード列データを成すY信号映像データDVYが供給される加減モジュロ演算部61と、鍵データDEYが供給される乱数発生部70と、を備えて構成されている。

加減モジュロ演算部61は、図11に示される加減モジュロ演算部61と同様のものであり、上述の如くにして、供給されるY信号映像データDVYを、10ビットワード列データを成す禁止コードを含まない暗号化Y信号映像データDXYに変換する。

乱数発生部70にあっては、レジスタ部71が、入力データに応答して、例えば、128ビット構成とされるレジスタ出力データDRZを送出し、それをDES暗号形成部72に供給する。このレジスタ部71には、初期入力データDITが供給される。

DES暗号形成部72には、鍵データDEYも供給され、DES暗号形成部72は、

レジスタ出力データDRZについての鍵データDEYによって定められる規則に従ったDES方式の暗号化を行い、例えば、128ビット構成とされる暗号データDEZを送出する。DES暗号形成部72から得られる暗号データDEZは、ビット分割部73に供給される。

ビット分割部73は、暗号データDEZを形成する128ビットを10ビットと118ビットとに分割し、10ビット構成の擬似乱数データDXAと118ビット構成の帰還用データDXBとを形成する。ビット分割部73から得られる擬似乱数データDXAは、乱数発生部70から送出されて、加減モジュロ演算部61に供給される。また、ビット分割部73から得られる帰還用データDXBは、ビット加算部74に供給される。

ビット加算部74には、加減モジュロ演算部61から送出される10ビットワード列データを成す暗号化Y信号映像データDXYも供給される。ビット加算部74は、ビット分割部73からの118ビット構成の帰還用データDXBに10ビットワード列データを成す暗号化Y信号映像データDXYをビット加算して、128ビット構成のデータDXB+DXYを形成して、それをレジスタ部71に入力データとして帰還する。それにより、レジスタ部71は、最初に、初期入力データDITに応じたレジスタ出力データDRZを送出し、その後は、ビット加算部74から得られるデータDXB+DXYに応じたレジスタ出力データDRZを送出することになる。

図19に示されるCデータ暗号化部42についての第4の具体構成例は、10ビットワード列データを成すC信号映像データDVCが供給される加減モジュロ演算部63と、鍵データDEYが供給される乱数発生部75と、を備えて構成されている。

加減モジュロ演算部63は、図12に示される加減モジュロ演算部63と同様のものであり、上述の如くにして、供給されるC信号映像データDVCを、10ビットワード列データを成す禁止コードを含まない暗号化C信号映像データDXCに変換する。

乱数発生部75は、図18に示される乱数発生部70と同様に、レジスタ部71、DES暗号形成部72、ビット分割部73及びビット加算部74とを含んで構成されている。但し、図18に示される乱数発生部70におけるビット加算部74が、ビット分割部73からの118ビット構成の帰還用データDXBと加減モジュロ演算部63から送出される10ビットワード列データを成す暗号化Y信号映像データDXYとが供給されて、128ビット構成のデータDXB+DXYを形成するのに対して、乱数発生部75におけるビット加算部74は、ビット分割部73からの118ビット構成の帰還用データDXBと加減モジュロ演算部63から送出される10ビットワード列データを成す暗号化C信号映像データDXCとが供給されて、128ビット構成のデータDXB+DXCを形成する。その他の動作は、図18に示される乱数発生部70と同様である。

上述の図18及び図19に示される具体構成例にあつては、加減モジュロ演算部6

1及び63に夫々連結された乱数発生部70及び75が、擬似乱数データDXAを発生してそれを加減モジュロ演算部61及び63に供給するものとされているが、乱数発生部70及び75を、擬似乱数データDXAに代えて、所定の乱数データを発生してそれを加減モジュロ演算部61及び63に供給するものとなすこともできる。

図20及び図21は、夫々、図7に示されるYデータ暗号化部41及びCデータ暗号化部42についての第5の具体構成例を示す。図20に示される第5の具体構成例が採用されたYデータ暗号化部41及び図21に示される第5の具体構成例が採用されたCデータ暗号化部42が用いられて、図6に示される暗号化部31が構成される場合には、その際に図6があらわす構成は、本願の請求の範囲における第3項、第4項、第5項または第7項に記載された発明に係るデータ伝送方法の第3の例が実施される、本願の請求の範囲における第11項、第12項、第13項または第15項に記載された発明に係るデータ伝送装置の第3の例を示すことになる。

図20に示されるYデータ暗号化部41についての第5の具体構成例は、10ビットワード列データを成すY信号映像データDVYが供給される加減モジュロ演算部61と、鍵データDEYが供給される乱数発生部76と、を備えて構成されている。

加減モジュロ演算部61は、図18に示される加減モジュロ演算部61と同様のものであり、上述の如くにして、供給されるY信号映像データDVYを、10ビットワード列データを成す禁止コードを含まない暗号化Y信号映像データDXYに変換する。

乱数発生部76は、図18に示される乱数発生部70と同様に、レジスタ部71、DES暗号形成部72、ビット分割部73及びビット加算部74とを含んで構成されている。但し、図18に示される乱数発生部70におけるビット加算部74が、ビット分割部73からの118ビット構成の帰還用データDXBと加減モジュロ演算部61から送出される10ビットワード列データを成す暗号化Y信号映像データDXYとが供給されて、128ビット構成のデータDXB+DXYを形成するのに対して、乱数発生部76におけるビット加算部74は、ビット分割部73からの118ビット構成の帰還用データDXBと加減モジュロ演算部61にも供給される10ビットワード列データを成すY信号映像データDVYとが供給されて、128ビット構成のデータDXB+DVYを形成する。その他の動作は、図18に示される乱数発生部70と同様である。

図21に示されるCデータ暗号化部42についての第5の具体構成例は、10ビットワード列データを成すC信号映像データDVCが供給される加減モジュロ演算部63と、鍵データDEYが供給される乱数発生部77と、を備えて構成されている。

加減モジュロ演算部63は、図19に示される加減モジュロ演算部63と同様のものであり、上述の如くにして、供給されるC信号映像データDVCを、10ビットワード列データを成す禁止コードを含まない暗号化C信号映像データDXCに変換する。

乱数発生部77は、図19に示される乱数発生部75と同様に、レジスタ部71、

27

D E S 暗号形成部 7 2 , ビット分割部 7 3 及びビット加算部 7 4 とを含んで構成されている。但し、図 1 9 に示される乱数発生部 7 5 におけるビット加算部 7 4 が、ビット分割部 7 3 からの 1 1 8 ビット構成の帰還用データ D X B と加減モジュロ演算部 6 3 から送出される 1 0 ビットワード列データを成す暗号化 C 信号映像データ D X C とが供給されて、1 2 8 ビット構成のデータ D X B + D X C を形成するのに対して、乱数発生部 7 7 におけるビット加算部 7 4 は、ビット分割部 7 3 からの 1 1 8 ビット構成の帰還用データ D X B と加減モジュロ演算部 6 3 にも供給される 1 0 ビットワード列データを成す C 信号映像データ D V C とが供給されて、1 2 8 ビット構成のデータ D X B + D V C を形成する。その他の動作は、図 1 9 に示される乱数発生部 7 5 と同様である。

上述の図 2 0 及び図 2 1 に示される具体構成例にあっては、加減モジュロ演算部 6 1 及び 6 3 に夫々連結された乱数発生部 7 6 及び 7 7 が、擬似乱数データ D X A を発生してそれを加減モジュロ演算部 6 1 及び 6 3 に供給するものとされているが、乱数発生部 7 6 及び 7 7 を、擬似乱数データ D X A に代えて、所定の乱数データを発生してそれを加減モジュロ演算部 6 1 及び 6 3 に供給するものとなすこともできる。

図 2 2 は、図 1 8 に示される Y データ暗号化部 4 1 の第 4 の具体構成例における乱数発生部 7 0 , 図 1 9 に示される C データ暗号化部 4 2 の第 4 の具体構成例における乱数発生部 7 5 , 図 2 0 に示される Y データ暗号化部 4 1 の第 5 の具体構成例における乱数発生部 7 6 、及び、図 2 1 に示される C データ暗号化部 4 2 の第 5 の具体構成例における乱数発生部 7 7 の夫々に代えて用いることができる乱数発生部の他の例を示す。

この図 2 2 に示される乱数発生部 7 0 ' にあっては、レジスタ部 7 1 ' が、初期入力データ D I T に応答して、例えば、1 2 8 ビット構成とされるレジスタ出力データ D R Z ' を送出し、それを A E S 暗号形成部 7 2 ' に供給する。A E S 暗号形成部 7 2 ' は、図 1 7 に示される乱数発生部 5 2 ' における A E S 暗号形成部 5 4 ' と同様のものである。

A E S 暗号形成部 7 2 ' には、鍵データ D E Y も供給され、A E S 暗号形成部 7 2 ' は、レジスタ出力データ D R Z ' についての鍵データ D E Y によって定められる規則に従った A E S 方式の暗号化を行い、例えば、1 2 8 ビット構成とされる暗号データ D E Z ' を送出する。A E S 暗号形成部 7 2 ' から得られる暗号データ D E Z ' は、ビット分割部 7 3 ' に供給される。

ビット分割部 7 3 ' は、暗号データ D E Z ' を形成する 1 2 8 ビットを 1 0 ビットと 1 1 8 ビットとに分割し、1 0 ビット構成の擬似乱数データ D X A ' と 1 1 8 ビット構成の帰還用データ D X B ' とを形成する。ビット分割部 7 3 ' から得られる擬似乱数データ D X A ' は、乱数発生部 7 0 ' から送出され、図 1 8 に示される乱数発生部 7 0 , 図 1 9 に示される乱数発生部 7 5 , 図 2 0 に示される乱数発生部 7 6 、及び、

図21に示される乱数発生部77の各々から送出される擬似乱数データDXAに代わるものとされる。

また、ビット分割部73'から得られる帰還用データDXB'は、ビット加算部74'に供給される。ビット加算部74'には、10ビットワード列データを成す暗号化Y信号映像データDXYも供給される。ビット加算部74'は、ビット分割部73'からの118ビット構成の帰還用データDXB'に10ビットワード列データを成す暗号化Y信号映像データDXYをビット加算して、128ビット構成のデータDXB' + DXYを形成して、それをレジスタ部71'に入力データとして帰還する。それにより、レジスタ部71'は、最初に、初期入力データDITに応じたレジスタ出力データDRZ'を送出し、その後は、ビット加算部74'から得られるデータDXB' + DXYに応じたレジスタ出力データDRZ'を送出することになる。

図23は、図6と組み合わされた状態をもって、本願の請求の範囲における第17項または第18項に記載された発明に係るデータ伝送方法の例が実施される、本願の請求の範囲における第25項または第26項に記載された発明に係るデータ伝送装置の例を示す。

図6については、既に説明したので、重複説明は省略する。

図23においては、図6におけるシリアルデータ形成部33から送出されて伝送された暗号化HD-SDI信号DXSが、パラレルデータ形成部81によって受けられる。パラレルデータ形成部81においては、暗号化HD-SDI信号DXSが等化部82に供給され、等化部82は、暗号化HD-SDI信号DXSに、それがケーブル伝送等により受ける主として高周波数成分の減衰に対処するための適正な等化处理を施し、等化处理が施された暗号化HD-SDI信号DXS'を形成する。等化部82から得られる暗号化HD-SDI信号DXS'は、NRZI変換部83及びクロック再生部84に供給される。クロック再生部84にあっては、暗号化HD-SDI信号DXS'についてのクロック信号CKを再生する。

クロック再生部84から得られるクロック信号CKは、NRZI変換部83に供給され、NRZI変換部83は、暗号化HD-SDI信号DXS'についてのクロック信号CKを用いてのNRZI変換を行う。それにより、NRZI変換部83からNRZI変換がなされた暗号化HD-SDI信号DXSCが送出されて、それがデスクランプリング部85に供給される。デスクランプリング部85には、クロック再生部84から得られるクロック信号CKも供給され、デスクランプリング部85は、暗号化HD-SDI信号DXSCにかけられたスクランブル処理を解除する。そして、デスクランプリング部85からスクランブル処理が解除された暗号化HD-SDI信号DXSDが導出されて、それがS/P変換部86及びワード同期信号形成部87に供給される。

ワード同期信号形成部87にあっては、クロック再生部84から得られるクロック信号CKも供給され、斯かるもとで、暗号化HD-SDI信号DXSDに含まれる、タイミ

ング基準コードデータSAVもしくはEAVを形成するタイミング識別コードとされる3FFh及び000hが、3FFh, 000h, 000hという順序で配列されてシリアルデータに変換された部分についての検出を行い、斯かる部分を検出したとき、ワード同期信号SWSを送出する。ワード同期信号形成部87から送出的るワード同期信号SWSは、S/P変換部86に供給される。S/P変換部86にあっては、クロック再生部84から得られるクロック信号CKも供給され、斯かるもとで、暗号化HD-SDI信号DXSDに対する、ワード同期信号SWSに従ったワード同期がとられたもとでのS/P変換処理を行う。このようなS/P変換処理により、暗号化HD-SDI信号DXSDを、各々が10ビットワード列データとされた暗号化Yデータ系列と暗号化P_B/P_Rデータ系列とが、タイミング基準コードデータSAV及びEAVについての同期がとられたもとでビット重畳されて得られるものとされる、暗号化20ビットワード列データDXPに変換する。

S/P変換部86から得られる暗号化20ビットワード列データDXPは、データ分離部88に供給される。データ分離部88にあっては、暗号化20ビットワード列データDXPを、重畳タイミングデータDAV、重畳補助データDAA及び暗号化映像データDXIに分割する。重畳タイミングデータDAVは、10ビットワード列を成すYデータ系列におけるタイミング基準コードデータEAV及びSAV、ライン番号データ、誤り検出符号データ等と、10ビットワード列を成すP_B/P_Rデータ系列におけるタイミング基準コードデータEAV及びSAV、ライン番号データ、誤り検出符号データ等とが、ワード同期がとられたもとでビット重畳されて得られる20ビットワード列データとされる。また、重畳補助データDAAは、10ビットワード列を成すYデータ系列における補助データと10ビットワード列を成すP_B/P_Rデータ系列における補助データとが、ワード同期がとられたもとでビット重畳されて得られる20ビットワード列データとされる。さらに、暗号化映像データDXIは、10ビットワード列を成す暗号化Yデータ系列における映像データ部を構成する暗号化Y信号映像データDXYと10ビットワード列を成す暗号化P_B/P_Rデータ系列における映像データ部を構成する暗号化C信号映像データDXCとが、ワード同期がとられたもとでビット重畳されて得られる20ビットワード列データとされる。

データ分離部88から得られる重畳タイミングデータDAV、重畳補助データDAA及び暗号化映像データDXIは、パラレルデータ形成部81から送出されて、復号化処理部89に供給される。復号化処理部89は、復号化部90と鍵データ送出部91とを含んで構成されている。

データ分離部88からの重畳タイミングデータDAV及び重畳補助データDAAは、復号化処理部89を素通りするものとされて、シリアルデータ形成部92に供給される。一方、データ分離部88からの暗号化映像データDXIは、復号化部90に供給される。鍵データ送出部91は、予め設定された鍵データDEYを復号化部90に供

給する。鍵データDEYは、図6に示される鍵データ送出部32から送出される鍵データDEYと同一の内容を有するものとされる。

復号化部90は、20ビットワード列データである暗号化映像データDXIに対して、鍵データDEYにより定められる規則に従った、例えば、DES方式、あるいは、他の方式による復号化処理を施し、暗号化映像データDXIに基づく重畳映像データDVIを、20ビットワード列データを成すものとして再生する。

図24は、復号化部90の具体構成例を示す。この図24に示される復号化部90の具体構成例にあつては、20ビットワード列データである暗号化映像データDXIがビット分割部100に供給される。ビット分割部100は、暗号化映像データDXIを、10ビットワード列を成す暗号化Y信号映像データDXYと10ビットワード列を成す暗号化C信号映像データDXCとに分割し、それらを個別に導出する。

ビット分割部100から得られる暗号化Y信号映像データDXY及び暗号化C信号映像データDXCは、Yデータ復号化部101及びCデータ復号化部102に夫々供給される。Yデータ復号化部101及びCデータ復号化部102の夫々には、鍵データ送出部91からの鍵データDEYも供給される。

Yデータ復号化部101は、10ビットワード列を成す暗号化Y信号映像データDXYに、鍵データDEYにより定められる規則に従ったDES方式による復号化処理を施し、暗号化Y信号映像データDXYに基づくY信号映像データDVYを10ビットワード列を成すものとして再生する。また、Cデータ復号化部102は、10ビットワード列を成す暗号化C信号映像データDXCに、鍵データDEYにより定められる規則に従ったDES方式による復号化処理を施し、復号化C信号映像データDXCに基づくC信号映像データDVCを10ビットワード列データを成すものとして再生する。

Yデータ復号化部101及びCデータ復号化部102から夫々得られる、10ビットワード列データを成すY信号映像データDVY及び10ビットワード列データを成すC信号映像データDVCは、ビット重畳部103に供給される。そして、ビット重畳部103にあつては、10ビットワード列データを成すY信号映像データDVYと10ビットワード列データを成すC信号映像データDVCとを重畳して、20ビットワード列データを成す重畳映像データDVIを形成し、それを復号化部90の出力データとして送出する。

復号化部90の出力データとされる重畳映像データDVIは、復号化処理部89から送出されて、シリアルデータ形成部92に供給される。シリアルデータ形成部92にあつては、データ分離部88から送出されて復号化処理部89を素通りした、各々が20ビットワード列データを成す重畳タイミングデータDAV及び重畳補助データDAAと、復号化処理部89から送出された20ビットワード列データを成す重畳映像データDVIとが、データ多重部104に供給される。

データ多重部104にあっては、重畳映像データDVI、重畳タイミングデータDAV及び重畳補助データDAAに多重化処理を施して、重畳映像データDVIと重畳タイミングデータDAVと重畳補助データDAAとを含んで成る20ビットワード列データDHPを再生する。このようにして、データ多重部104において再生される20ビットワード列データDHPは、P/S変換部105に供給される。

P/S変換部105にあっては、20ビットワード列データDHPにP/S変換処理を施して、20ビットワード列データDHPに基づくシリアルデータDHSDを再生し、それをスクランプリング部106に供給する。

スクランプリング部106は、シリアルデータDHSDにスクランブル処理を施し、スクランブル処理がかけられたシリアルデータDHSCを形成して、それをNRZI変換部108に供給する。NRZI変換部108は、スクランブル処理がかけられたシリアルデータDHSCについてのNRZI変換を行う。それにより、NRZI変換部108において、HD-SDI信号DHSが再生され、それがシリアルデータ形成部92から導出される。

図25及び図26は、夫々、図24に示されるYデータ復号化部101及びCデータ復号化部102についての第1の具体構成例を示す。図25に示される第1の具体構成例が採用されたYデータ復号化部101及び図26に示される第1の具体構成例が採用されたCデータ復号化部102が用いられて、図23に示される復号化部90が構成される場合には、その際に図6と図23との組合せがあらわす構成は、本願の請求の範囲における第19項、第20項、第21項または第22項に記載された発明に係るデータ伝送方法の例が実施される、本願の請求の範囲における第27項、第28項、第29項または第30項に記載された発明に係るデータ伝送装置の例を示すことになる。

図25に示されるYデータ復号化部101についての第1の具体構成例は、10ビットワード列データを成す暗号化Y信号映像データDXYが第1の読出アドレスデータとして供給されるメモリ部111と、鍵データDEYが供給される乱数発生部112と、を備えて構成されている。

乱数発生部112は、図8に示される乱数発生部52と同様に、レジスタ部53、DES暗号形成部54及びビット取出部55を含んで構成され、擬似乱数データDXAを送出して、それをメモリ部111に、第2の読出アドレスデータとして供給する。

メモリ部111にあっては、禁止コード000h~003h及び3FCh~3FFhが除かれた10ビットコードを有した $1024 - 8 = 1016$ 個の10ビットワードデータが格納されている。これらの1016個の10ビットワードデータは、夫々が有する10ビットコードが、メモリ部111に第1の読出アドレスデータとして供給される暗号化Y信号映像データDXYを形成する10ビットワードの夫々が有する10ビットコードと、1対1の特定の対応関係を取り、その特定の対応関係のもとに、

暗号化Y信号映像データDXYに応じてメモリ部111から読み出されるとともに、斯かる特定の対応関係が、メモリ部111に第2の読出アドレスデータとして供給される擬似乱数データDXAに応じて変化するものとされる。

上述の如くにしてメモリ部111から読み出される10ビットワードデータは、順次配列されて、10ビットワード列データを成すY信号映像データDVYを形成する。

図26に示されるCデータ復号化部102についての第1の具体構成例は、10ビットワード列データを成す暗号化C信号映像データDXCが第1の読出アドレスデータとして供給されるメモリ部116と、鍵データDEYが供給される乱数発生部117と、を備えて構成されている。

乱数発生部117は、図25に示される乱数発生部112と同様のものであり、レジスタ部53、DES暗号形成部54及びビット取出部55を含んで構成されていて、擬似乱数データDXAを送出して、それをメモリ部116に、第2の読出アドレスデータとして供給する。

メモリ部116にも、禁止コード000h~003h及び3FCh~3FFhが除かれた10ビットコードを有した1024-8=1016個の10ビットワードデータが格納されている。そして、これらの1016個の10ビットワードデータは、夫々が有する10ビットコードが、メモリ部116に第1の読出アドレスデータとして供給される暗号化C信号映像データDXCを形成する10ビットワードの夫々が有する10ビットコードと、1対1の特定の対応関係を取り、その特定の対応関係のもとに、暗号化C信号映像データDXCに応じてメモリ部116から読み出されるとともに、斯かる特定の対応関係が、メモリ部116に第2の読出アドレスデータとして供給される擬似乱数データDXAに応じて変化するものとされる。

メモリ部116から読み出される10ビットワードデータは、順次配列されて、10ビットワード列データを成すC信号映像データDVCを形成する。

上述の図25及び図26に示される具体構成例にあっては、メモリ部111及び116に夫々連結された乱数発生部112及び117が、擬似乱数データDXAを発生してそれをメモリ部111及び116に供給するものとされているが、乱数発生部112及び117を、擬似乱数データDXAに代えて、所定の乱数データを発生してそれをメモリ部111及び116に供給するものとなすこともできる。

図27及び図28は、夫々、図24に示されるYデータ復号化部101及びCデータ復号化部102についての第2の具体構成例を示す。図27に示される第2の具体構成例が採用されたYデータ復号化部101及び図28に示される第2の具体構成例が採用されたCデータ復号化部102が用いられて、図23に示される復号化部90が構成される場合には、その際に図6と図23との組合せがあらわす構成は、本願の請求の範囲における第19項、第20項、第21項または第23項に記載された発明に係るデータ伝送方法の第1の例が実施される、本願の請求の範囲における第27項、

第28項、第29項または第31項に記載された発明に係るデータ伝送装置の第1の例を示すことになる。

図27に示されるYデータ復号化部101についての第2の具体構成例は、10ビットワード列データを成す暗号化Y信号映像データDXYが供給される加減モジュロ演算部121と、鍵データDEYが供給される乱数発生部122と、を備えて構成されている。

乱数発生部122は、図25に示される乱数発生部112と同様のものであり、レジスタ部53、DES暗号形成部54及びビット取出部55を含んで構成されていて、擬似乱数データDXAを送出して、それを加減モジュロ演算部121に供給する。

加減モジュロ演算部121は、供給される暗号化Y信号映像データDXYをY信号映像データDVYに変換する。この加減モジュロ演算部121にあっては、暗号化Y信号映像データDXYに対して、擬似乱数データDXAに応じた、加減モジュロ演算を行い、加減モジュロ演算の結果に基づいて定められる変換されたコードをY信号映像データDVYについてのコードとする。それにより、暗号化Y信号映像データDXYが、Y信号映像データDVYに変換されることになる。

ここでは、暗号化Y信号映像データDXYが10ビットワード列データを成すものとされているので、10ビットコードについて考えると、10ビットコードは、000hから3FFhまで、1024個ある。そこで、これらの1024個のコードに、000hから3FFhまで順番に1から1024までのコード位置番号を付すこととする。上述の加減モジュロ演算は、このようなコード位置番号が設定されたもとにおいて、Y信号映像データDVYを形成する10ビットワードがとるべき10ビットコードのコード位置番号を定めるものとされる。

加減モジュロ演算における演算式は、具体的には、暗号化Y信号映像データDXYがとる情報コードのコード位置番号をCi、Y信号映像データDVYがとるべき情報コードのコード位置番号をMi、擬似乱数データDXAがとる10ビットコードのコード位置番号をEiとし、さらに、Y信号映像データDVYがとり得る情報コードの範囲の一端側に配される禁止コードの個数をN1、Y信号映像データDVYがとり得る情報コードの個数をN2として、下記の〔数2〕によりあらわすことができる。

〔数2〕

$$M_i = \{ (C_i - N_1) - E_i \} \bmod N_2 + N_1$$

但し、 $\{ (C_i - N_1) - E_i \} \bmod N_2$ は、 $\{ (C_i - N_1) - E_i \}$ をN2で除した余りを意味する。

Y信号映像データDVYは10ビットワード列データを成すものであるため、N1は、禁止コード000h～003hの個数であり、従って、4となり、また、N2は、10ビットコードの総個数から禁止コードの個数を減じた個数、即ち、 $1024 - 8 = 1016$ となる。

〔数2〕によりあらわされる演算式においては、 C_i から $N-1$ を減じる減算が行われて、それにより、暗号化Y信号映像データ DX_Y がとる情報コードのコード位置番号が、4だけ小なるコード位置番号に変換される。続いて、斯かる変換により得られるコード位置番号から、擬似乱数データ DX_A がとる10ビットコードのコード位置番号が引かれた後、それを1016で除した余りが求められるモジュロ演算が行われる。そして、求められた余りに4を加える加算が行われ、それにより得られるコード位置番号が、Y信号映像データ DV_Y がとるべき情報コードのコード位置番号 M_i とされる。

そして、加減モジュロ演算部121にあっては、このようにして加減モジュロ演算の結果得られるコード位置番号 M_i に対応する10ビットコードが、Y信号映像データ DV_Y がとる情報コードとされる。

図28に示されるCデータ復号化部102についての第2の具体構成例は、10ビットワード列データを成す暗号化C信号映像データ DX_C が供給される加減モジュロ演算部123と、鍵データ DE_Y が供給される乱数発生部124と、を備えて構成されている。

乱数発生部124は、図27に示される乱数発生部122と同様のものであり、レジスタ部53、DES暗号形成部54及びビット取出部55を含んで構成されていて、擬似乱数データ DX_A を送出して、それを加減モジュロ演算部123に供給する。

加減モジュロ演算部123は、供給される暗号化C信号映像データ DX_C をC信号映像データ DV_C に変換する。この加減モジュロ演算部123にあっては、暗号化C信号映像データ DX_C に対して、擬似乱数データ DX_A に応じた、加減モジュロ演算を行い、加減モジュロ演算の結果に基づいて定められる変換されたコードをC信号映像データ DV_C についてのコードとする。この暗号化C信号映像データ DX_C に対する加減モジュロ演算は、上述の図27に示される加減モジュロ演算部121によって行われる暗号化Y信号映像データ DX_Y に対しての加減モジュロ演算と同様にして行われる。その結果、暗号化C信号映像データ DX_C が、C信号映像データ DV_C に変換されることになる。

上述の図27及び図28に示される具体構成例にあっては、加減モジュロ演算部121及び123に夫々連結された乱数発生部122及び124が、擬似乱数データ DX_A を発生してそれを加減モジュロ演算部121及び123に供給するものとされているが、乱数発生部122及び124を、擬似乱数データ DX_A に代えて、所定の乱数データを発生してそれを加減モジュロ演算部121及び123に供給するものとなすこともできる。

図29及び図30は、夫々、図24に示されるYデータ復号化部101及びCデータ復号化部102についての第3の具体構成例を示す。図29に示される第3の具体構成例が採用されたYデータ復号化部101及び図30に示される第3の具体構成例

が採用されたCデータ復号化部102が用いられて、図23に示される復号化部90が構成される場合には、その際に図6と図23との組合せがあらわす構成は、本願の請求の範囲における第19項、第20項、第21項または第24項に記載された発明に係るデータ伝送方法の例が実施される、本願の請求の範囲における第27項、第28項、第29項または第32項に記載された発明に係るデータ伝送装置の例を示すことになる。

図29に示されるYデータ復号化部101についての第3の具体構成例は、Y信号映像データDVYが、禁止コードを情報コードの範囲外に配される000h~003h及び3FCh~3FFhとするもとで形成されたものでなく、情報コードと禁止コードとが混在する状態のもとで、情報コードのみが用いられて形成されたものとされる場合に用いられる。そして、図29に示されるYデータ復号化部101についての第3の具体構成例は、上述の図27に示されるYデータ復号化部101についての第2の具体構成例に、加減モジュロ演算部121の出力側に配されるメモリ部126が追加されたものに該当するものとして構成される。

加減モジュロ演算部121及び乱数発生部122は、図27に示されるYデータ復号化部101についての第2の具体構成例における加減モジュロ演算部121及び乱数発生部122と同様に動作し、加減モジュロ演算部121から、暗号化Y信号映像データDXYに基づくY信号映像データDVY'が送出される。このY信号映像データDVY'は、図27に示されるYデータ復号化部101についての第2の具体構成例における加減モジュロ演算部121から送出されるY信号映像データDVYに相当するものであり、禁止コードの範囲が情報コードの範囲外に配されたことになるものとされている。

加減モジュロ演算部121から送出されるY信号映像データDVY'は、メモリ部126に供給される。メモリ部126においては、Y信号映像データDVY'の書込みと読出しとが行われ、メモリ部126から、Y信号映像データDVY'に基づくY信号映像データDVYが送出される。その際、Y信号映像データDVY'の書込みにあたっては、Y信号映像データDVY'を形成する各10ビットワードが、それがとる10ビットコードに応じて定められた書込アドレスをもって書き込まれ、また、Y信号映像データDVY'の読出しにあたっては、Y信号映像データDVY'を形成する各10ビットワードが、書込アドレスと1対1の特定の対応関係を有するものとされた読出アドレスをもって読み出される。そして、このような書込アドレスと読出アドレスとの間の1対1の特定の対応関係は、禁止コードに割り当てられる書込アドレスが、情報コードに割り当てられる読出アドレスの範囲内に、分散される読出アドレスに対応するものとなるようにされる。

それにより、メモリ部126に書き込まれたY信号映像データDVY'が読み出されることによりメモリ部126から送出されるY信号映像データDVYが、情報コー

ドと禁止コードとが混在する状態のもとで、情報コードのみが用いられて形成されたものとされる。

このようにして、図29に示されるYデータ復号化部101についての第3の具体構成例にあつては、暗号化Y信号映像データDXYが加減モジュロ演算部121によってY信号映像データDXY'に変換され、さらに、メモリ部126によってY信号映像データDVY'についての変換が行われて、Y信号映像データDVYが得られる。

図30に示されるCデータ復号化部102についての第3の具体構成例は、C信号映像データDVCが、禁止コードを情報コードの範囲外に配される000h~003h及び3FCh~3FFhとするもとで形成されたものでなく、情報コードと禁止コードとが混在する状態のもとで、情報コードのみが用いられて形成されたものとされる場合に用いられる。そして、図30に示されるCデータ復号化部102についての第3の具体構成例は、図28に示されるCデータ復号化部102についての第2の具体構成例に、加減モジュロ演算部123の出力側に配されるメモリ部127が追加されたものに該当するものとして構成される。

加減モジュロ演算部123及び乱数発生部124は、図28に示されるCデータ復号化部102についての第2の具体構成例における加減モジュロ演算部123及び乱数発生部124と同様に動作し、加減モジュロ演算部123から、暗号化C信号映像データDXCに基づくC信号映像データDVC'が送出される。このC信号映像データDVC'は、図28に示されるCデータ復号化部102についての第2の具体構成例における加減モジュロ演算部123から送出されるC信号映像データDVCに相当するものであり、禁止コードの範囲が情報コードの範囲外に配されたことになるものとされている。

加減モジュロ演算部123から送出されるC信号映像データDVC'は、メモリ部127に供給される。メモリ部127においては、C信号映像データDVC'の書込みと読出しとが行われ、メモリ部127から、C信号映像データDVC'に基づくC信号映像データDVCが送出される。その際、C信号映像データDVC'の書込みにあつては、C信号映像データDVC'を形成する各10ビットワードが、それがとる10ビットコードに応じて定められた書込アドレスをもって書き込まれ、また、C信号映像データDVC'の読出しにあつては、C信号映像データDVC'を形成する各10ビットワードが、書込アドレスと1対1の特定の対応関係を有するものとされた読出アドレスをもって読み出される。そして、このような書込アドレスと読出アドレスとの間の1対1の特定の対応関係は、禁止コードに割り当てられる書込アドレスが、情報コードに割り当てられる読出アドレスの範囲内に、分散される読出アドレスに対応するものとなるようにされる。

それにより、メモリ部127に書き込まれたC信号映像データDVC'が読み出されることによりメモリ部127から送出されるC信号映像データDVCが、情報コー

ドと禁止コードとが混在する状態のもとで、情報コードのみが用いられて形成されたものとされる。

このようにして、図30に示されるCデータ復号化部102についての第3の具体構成例にあつては、暗号化C信号映像データDXCが加減モジュロ演算部123によってC信号映像データDVC'に変換され、さらに、メモリ部127によってC信号映像データDVC'についての変換が行われて、C信号映像データDVCが得られる。

上述の図29及び図30に示される具体構成例にあつては、加減モジュロ演算部121及び123に夫々連結された乱数発生部122及び124が、擬似乱数データDXAを発生してそれを加減モジュロ演算部121及び123に供給するものとされているが、乱数発生部122及び124を、擬似乱数データDXAに代えて、所定の乱数データを発生してそれを加減モジュロ演算部121及び123に供給するものとなすこともできる。

図31は、図25に示されるYデータ暗号化部101の第1の具体構成例における乱数発生部112，図26に示されるCデータ暗号化部102の第1の具体構成例における乱数発生部117，図27及び図29に夫々示されるYデータ暗号化部101の第2及び第3の具体構成例の各々における乱数発生部122、及び、図28及び図30に夫々示されるCデータ暗号化部102の第2及び第3の具体構成例の各々における乱数発生部124の夫々に代えて用いることができる乱数発生部の他の例を示す。

この図31に示される乱数発生部112'は、図17に示される乱数発生部52'と同様に構成されるものとされ、それについての重複説明は省略されるが、この乱数発生部112'から送出される擬似乱数データDXA'が、図25に示される乱数発生部112，図26に示される乱数発生部117，図27及び図29の夫々に示される乱数発生部122、及び、図28及び図30の夫々に示される乱数発生部124の各々から送出される擬似乱数データDXAに代わるものとされる。

図32及び図33は、夫々、図24に示されるYデータ復号化部101及びCデータ復号化部132についての第4の具体構成例を示す。図32に示される第4の具体構成例が採用されたYデータ復号化部101及び図33に示される第4の具体構成例が採用されたCデータ復号化部102が用いられて、図23に示される復号化部90が構成される場合には、その際に図6と図23との組合せがあらわす構成は、本願の請求の範囲における第19項，第20項，第21項または第22項に記載された発明に係るデータ伝送方法の第2の例が実施される、本願の請求の範囲における第27項，第28項，第29項または第30項に記載された発明に係るデータ伝送装置の第2の例を示すことになる。

図32に示されるYデータ復号化部101についての第4の具体構成例は、10ビットワード列データを成す暗号化Y信号映像データDXYが供給される加減モジュロ演算部121と、鍵データDEYが供給される乱数発生部130と、を備えて構成さ

れている。

加減モジュロ演算部121は、図27に示される加減モジュロ演算部121と同様のものであり、上述の如くにして、供給される暗号化Y信号映像データDXYを、10ビットワード列データを成すY信号映像データDVYに変換する。

乱数発生部130にあっては、レジスタ部131が、入力データに応答して、例えば、128ビット構成とされるレジスタ出力データDRZを送出し、それをDES暗号形成部132に供給する。このレジスタ部131には、初期入力データDITが供給される。

DES暗号形成部132には、鍵データDEYも供給され、DES暗号形成部132は、レジスタ出力データDRZについての鍵データDEYによって定められる規則に従ったDES方式の暗号化を行い、例えば、128ビット構成とされる暗号データDEZを送出する。DES暗号形成部132から得られる暗号データDEZは、ビット分割部133に供給される。

ビット分割部133は、暗号データDEZを形成する128ビットを10ビットと118ビットとに分割し、10ビット構成の擬似乱数データDXAと118ビット構成の帰還用データDXBとを形成する。ビット分割部133から得られる擬似乱数データDXAは、乱数発生部130から送出されて、加減モジュロ演算部121に供給される。また、ビット分割部133から得られる帰還用データDXBは、ビット加算部134に供給される。

ビット加算部134には、加減モジュロ演算部121にも供給される10ビットワード列データを成す暗号化Y信号映像データDXYも供給される。ビット加算部134は、ビット分割部133からの118ビット構成の帰還用データDXBに10ビットワード列データを成す暗号化Y信号映像データDXYをビット加算して、128ビット構成のデータDXB+DXYを形成して、それをレジスタ部131に入力データとして帰還する。それにより、レジスタ部131は、最初に、初期入力データDITに応じたレジスタ出力データDRZを送出し、その後は、ビット加算部134から得られるデータDXB+DXYに応じたレジスタ出力データDRZを送出することになる。

図33に示されるCデータ復号化部102についての第4の具体構成例は、10ビットワード列データを成す暗号化C信号映像データDXCが供給される加減モジュロ演算部123と、鍵データDEYが供給される乱数発生部135と、を備えて構成されている。

加減モジュロ演算部123は、図28に示される加減モジュロ演算部123と同様のものであり、上述の如くにして、供給される暗号化C信号映像データDXCを、10ビットワード列データを成すC信号映像データDVCに変換する。

乱数発生部135は、図32に示される乱数発生部130と同様に、レジスタ部1

31, DES暗号形成部132, ビット分割部133及びビット加算部134とを含んで構成されている。但し、図32に示される乱数発生部130におけるビット加算部134が、ビット分割部133からの118ビット構成の帰還用データDXBと加減モジュロ演算部121にも供給される10ビットワード列データを成す暗号化Y信号映像データDXYとが供給されて、128ビット構成のデータDXB+DXYを形成するのに対して、乱数発生部135におけるビット加算部134は、ビット分割部133からの118ビット構成の帰還用データDXBと加減モジュロ演算部123にも供給される10ビットワード列データを成す暗号化C信号映像データDXCとが供給されて、128ビット構成のデータDXB+DXCを形成する。その他の動作は、図32に示される乱数発生部130と同様である。

上述の図32及び図33に示される具体構成例にあっては、加減モジュロ演算部121及び123に夫々連結された乱数発生部130及び135が、擬似乱数データDXAを発生してそれを加減モジュロ演算部121及び123に供給するものとされているが、乱数発生部130及び135を、擬似乱数データDXAに代えて、所定の乱数データを発生してそれを加減モジュロ演算部121及び123に供給するものとなすこともできる。

図34及び図35は、夫々、図24に示されるYデータ復号化部101及びCデータ復号化部102についての第5の具体構成例を示す。図34に示される第5の具体構成例が採用されたYデータ復号化部101及び図35に示される第5の具体構成例が採用されたCデータ復号化部102が用いられて、図23に示される復号化部90が構成される場合には、その際に図6と図23との組合せがあらわす構成は、本願の請求の範囲における第19項、第20項、第21項または第22項に記載された発明に係るデータ伝送方法の第3の例が実施される、本願の請求の範囲における第27項、第28項、第29項または第30項に記載された発明に係るデータ伝送装置の第3の例を示すことになる。

図34に示されるYデータ復号化部101についての第5の具体構成例は、10ビットワード列データを成す暗号化Y信号映像データDXYが供給される加減モジュロ演算部121と、鍵データDEYが供給される乱数発生部136と、を備えて構成されている。

加減モジュロ演算部121は、図32に示される加減モジュロ演算部121と同様のものであり、上述の如くにして、供給される暗号化Y信号映像データDXYを、10ビットワード列データを成すY信号映像データDVYに変換する。

乱数発生部136は、図32に示される乱数発生部130と同様に、レジスタ部131, DES暗号形成部132, ビット分割部133及びビット加算部134とを含んで構成されている。但し、図32に示される乱数発生部130におけるビット加算部134が、ビット分割部133からの118ビット構成の帰還用データDXBと加

減モジュロ演算部121にも供給される10ビットワード列データを成す暗号化Y信号映像データDX Yとが供給されて、128ビット構成のデータDX B+DX Yを形成するのに対して、乱数発生部136におけるビット加算部134は、ビット分割部133からの118ビット構成の帰還用データDX Bと加減モジュロ演算部121から送出される10ビットワード列データを成すY信号映像データDV Yとが供給されて、128ビット構成のデータDX B+DV Yを形成する。その他の動作は、図32に示される乱数発生部130と同様である。

図35に示されるCデータ復号化部102についての第5の具体構成例は、10ビットワード列データを成す暗号化C信号映像データDX Cが供給される加減モジュロ演算部123と、鍵データDE Yが供給される乱数発生部137と、を備えて構成されている。

加減モジュロ演算部123は、図33に示される加減モジュロ演算部123と同様のものであり、上述の如くにして、供給される暗号化C信号映像データDX Cを、10ビットワード列データを成すC信号映像データDV Cに変換する。

乱数発生部137は、図33に示される乱数発生部135と同様に、レジスタ部131、DES暗号形成部132、ビット分割部133及びビット加算部134とを含んで構成されている。但し、図33に示される乱数発生部135におけるビット加算部134が、ビット分割部133からの118ビット構成の帰還用データDX Bと加減モジュロ演算部123にも供給される10ビットワード列データを成す暗号化C信号映像データDX Cとが供給されて、128ビット構成のデータDX B+DX Cを形成するのに対して、乱数発生部137におけるビット加算部134は、ビット分割部133からの118ビット構成の帰還用データDX Bと加減モジュロ演算部123から送出される10ビットワード列データを成すC信号映像データDV Cとが供給されて、128ビット構成のデータDX B+DV Cを形成する。その他の動作は、図33に示される乱数発生部135と同様である。

上述の図34及び図35に示される具体構成例にあつては、加減モジュロ演算部121及び123に夫々連結された乱数発生部136及び137が、擬似乱数データDX Aを発生してそれを加減モジュロ演算部121及び123に供給するものとされているが、乱数発生部136及び137を、擬似乱数データDX Aに代えて、所定の乱数データを発生してそれを加減モジュロ演算部121及び123に供給するものとなすこともできる。

図36は、図32に示されるYデータ暗号化部101の第4の具体構成例における乱数発生部130、図33に示されるCデータ暗号化部102の第4の具体構成例における乱数発生部135、図34に示されるYデータ暗号化部101の第5の具体構成例における乱数発生部136、及び、図35に示されるCデータ暗号化部102の第5の具体構成例における乱数発生部137の夫々に代えて用いることができる乱数

発生部の他の例を示す。

この図36に示される乱数発生部130'にあっては、レジスタ部131'が、初期入力データDITに応答して、例えば、128ビット構成とされるレジスタ出力データDRZ'を送出し、それをAES暗号形成部132'に供給する。AES暗号形成部132'は、図17に示される乱数発生部52'におけるAES暗号形成部54'と同様のものである。

AES暗号形成部132'には、鍵データDEYも供給され、AES暗号形成部132'は、レジスタ出力データDRZ'についての鍵データDEYによって定められる規則に従ったAES方式の暗号化を行い、例えば、128ビット構成とされる暗号データDEZ'を送出する。AES暗号形成部132'から得られる暗号データDEZ'は、ビット分割部133'に供給される。

ビット分割部133'は、暗号データDEZ'を形成する128ビットを10ビットと118ビットとに分割し、10ビット構成の擬似乱数データDXA'と118ビット構成の帰還用データDXB'とを形成する。ビット分割部133'から得られる擬似乱数データDXA'は、乱数発生部130'から送出され、図32に示される乱数発生部130、図33に示される乱数発生部135、図34に示される乱数発生部136、及び、図35に示される乱数発生部137の各々から送出される擬似乱数データDXAに代わるものとされる。

また、ビット分割部133'から得られる帰還用データDXB'は、ビット加算部134'に供給される。ビット加算部134'には、10ビットワード列データを成す暗号化Y信号映像データDXYも供給される。ビット加算部134'は、ビット分割部133'からの118ビット構成の帰還用データDXB'に10ビットワード列データを成す暗号化Y信号映像データDXYをビット加算して、128ビット構成のデータDXB'+DXYを形成して、それをレジスタ部131'に入力データとして帰還する。それにより、レジスタ部131'は、最初に、初期入力データDITに応じたレジスタ出力データDRZ'を送出し、その後は、ビット加算部134'から得られるデータDXB'+DXYに応じたレジスタ出力データDRZ'を送出することになる。

なお、上述の例にあっては、図6に示される、暗号化処理が行われるデータ伝送装置から、図23に示される、復号化処理が行われるデータ伝送装置へのデータ伝送が、シリアルデータが伝送される形態をもって行われるが、本願の請求の範囲に記載された発明に係るデータ伝送方法及びデータ伝送装置は、暗号化処理が行われるデータ伝送装置から、図23に示される、復号化処理が行われるデータ伝送装置へのデータ伝送が、パラレルデータが伝送される形態をもって行われる場合にも、適用することができるものである。

産業上の利用可能性

以上の説明から明らかな如く、本願の請求の範囲における第1項から第8項までのいずれかに記載された発明に係るデータ伝送方法、もしくは、本願の請求の範囲における第9項から第16項までのいずれかに記載された発明に係るデータ伝送装置によれば、デジタル情報データと禁止コードが用いられたタイミング基準コードデータとを含んだワード列データにおけるデジタル情報データに、禁止コードを発生させない暗号化処理が施されて、禁止コードを含まない暗号化デジタル情報データが得られるとともに、その暗号化デジタル情報データとタイミング基準コードデータとを含んだ暗号化ワード列データが形成され、その暗号化ワード列データが伝送されるべく送出される。それゆえ、送出される暗号化ワード列データに基づく暗号化シリアルデータが形成される場合において、その暗号化シリアルデータが、不所望な禁止コードがシリアルデータに変換された部分を含むものとなる事態はもたらされない。

従って、本願の請求の範囲における第1項から第8項までのいずれかに記載された発明に係るデータ伝送方法、もしくは、本願の請求の範囲における第9項から第16項までのいずれかに記載された発明に係るデータ伝送装置が、例えば、HD-SDI信号の如くの、タイミング識別用コードを含む複数のコードが禁止コードとされて形成されたデジタル情報データとタイミング識別用コードが用いられたタイミング基準コードデータとを含んだワード列データに基づくシリアルデータに応じた、デジタル情報データに暗号化処理を施して形成した暗号化シリアルデータを伝送するデータ暗号化伝送に適用されるときには、斯かるデータ暗号化伝送を、伝送される暗号化シリアルデータに不所望な禁止コードがシリアルデータに変換された部分が含まれてしまう事態をまねくことなく行えることになる。

また、本願の請求の範囲における第17項から第24項までのいずれかに記載された発明に係るデータ伝送方法、もしくは、本願の請求の範囲における第25項から第32項までのいずれかに記載された発明に係るデータ伝送装置によれば、デジタル情報データと禁止コードが用いられたタイミング基準コードデータとを含んだワード列データにおけるデジタル情報データに、禁止コードを発生させない暗号化処理が施されて、禁止コードを含まない暗号化デジタル情報データが得られるとともに、その暗号化デジタル情報データとタイミング基準コードデータとを含んだ暗号化ワード列データが形成され、その暗号化ワード列データが伝送されるべく送出され、さらに、送出された暗号化ワード列データから取り出された暗号化デジタル情報データに復号化処理が施されて、再生デジタル情報データが得られ、それとタイミング基準コードデータとを含んだ再生ワード列データが形成される。それゆえ、送出される暗号化ワード列データに基づく暗号化シリアルデータが形成される場合において、その暗号化シリアルデータが、不所望な禁止コードがシリアルデータに変換された部分を含むものとなる事態はもたらされず、また、伝送された暗号化シリアルデータに

基づいて元のシリアルデータが再生される場合において、元のシリアルデータの再生が適正に行われる。そして、送出された暗号化ワード列データから取り出された暗号化デジタル情報データに対する復号化処理を含んだ処理により、送出された暗号化ワード列データに基づく再生ワード列データの形成が確実に行われる。

従って、本願の請求の範囲における第 1 7 項から第 2 4 項までのいずれかに記載された発明に係るデータ伝送方法、もしくは、本願の請求の範囲における第 2 5 項から第 3 2 項までのいずれかに記載された発明に係るデータ伝送装置が、例えば、HD-SDI 信号の如くの、タイミング識別用コードを含む複数のコードが禁止コードとされて形成されたデジタル情報データとタイミング識別用コードが用いられたタイミング基準コードデータとを含んだワード列データに基づくシリアルデータに応じた、デジタル情報データに暗号化処理を施して形成した暗号化シリアルデータを伝送し、伝送された暗号化シリアルデータに基づいて元のシリアルデータを再生するデータ暗号化伝送に適用されるときには、斯かるデータ暗号化伝送を、伝送される暗号化シリアルデータに不所望な禁止コードがシリアルデータに変換された部分が含まれてしまう事態をまねくことなく、かつ、元のシリアルデータを確実に再生できるもとで行えることになる。

請 求 の 範 囲

1. タイミング識別用コードを含む複数のコードが、情報をあらわす情報コードとしては使用されない禁止コードとされて形成されたデジタル情報データと、上記タイミング識別用コードが用いられたタイミング基準コードデータと、を含んだワード列データにおける上記デジタル情報データに、上記禁止コードを発生させない暗号化処理を施して、上記禁止コードを含まない暗号化デジタル情報データを得るとともに、該暗号化デジタル情報データと上記タイミング基準コードデータとを含んだ暗号化ワード列データを形成し、該暗号化ワード列データを伝送すべく送出するデータ伝送方法。
2. デジタル情報データとタイミング基準コードデータとを含んだワード列データに、タイミング基準コードデータを分離するデータ分離処理を施して、デジタル情報データを得、該デジタル情報データに基づく暗号化デジタル情報データを得ることを特徴とする請求の範囲第1項記載のデータ伝送方法。
3. デジタル情報データと乱数データもしくは擬似乱数データとに、禁止コードを演算出力として発生することがない演算処理を施し、該演算処理により得られる演算出力を取り出して暗号化デジタル情報データを得ることを特徴とする請求の範囲第1項記載のデータ伝送方法。
4. 入力データに対応して鍵データに応じた規則に従って暗号データを出力する暗号形成部が出力する上記暗号データの一部を取り出すことにより、乱数データもしくは擬似乱数データを得ることを特徴とする請求の範囲第3項記載のデータ伝送方法。
5. 入力データに対応して鍵データに応じた規則に従って暗号データを出力する暗号形成部に、上記暗号データの全部もしくは部分を入力データとして戻す帰還をかけるとともに、上記暗号形成部が出力する暗号データの一部を取り出すことにより、乱数データもしくは擬似乱数データを得ることを特徴とする請求の範囲第3項記載のデータ伝送方法。
6. デジタル情報データと乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記禁止コードを含まない複数の設定ワードデータが格納されたメモリ手段を用意し、上記デジタル情報データを構成する複数の情報ワードデータにより上記メモリ手段の読出アドレスを制御して、上記複数の設定ワードデータを、上記複数の情報ワードデータと予め定められた対応

関係を有するものとして読み出すとともに、上記乱数データもしくは擬似乱数データに応じて上記予め定められた対応関係を変化させることにより行い、暗号化デジタル情報データを上記メモリ手段からの読出出力データとして得ることを特徴とする請求の範囲第3項記載のデータ伝送方法。

7. デジタル情報データと乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記デジタル情報データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータ、及び、上記デジタル情報データがとり得る情報コードの個数をあらわすデータを用いて行う、上記デジタル情報データと上記乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算となすことを特徴とする請求の範囲第3項記載のデータ伝送方法。

8. デジタル情報データと乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記デジタル情報データについての、メモリ手段への書込み及び該メモリ手段からの読出しによる、とり得る情報コードの範囲の一方の端部側に禁止コードが位置することになるワード位置変換ワード列データへの変換、及び、該ワード位置変換ワード列データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータと、上記ワード位置変換ワード列データがとり得る情報コードの個数をあらわすデータと、を用いて行う、上記ワード位置変換ワード列データと上記乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算、となすことを特徴とする請求の範囲第3項記載のデータ伝送方法。

9. タイミング識別用コードを含む複数のコードが、情報をあらわす情報コードとしては使用されない禁止コードとされて形成されたデジタル情報データと、上記タイミング識別用コードが用いられたタイミング基準コードデータと、を含んだワード列データにおける上記デジタル情報データに、上記禁止コードを発生させない暗号化処理を施して、上記禁止コードを含まない暗号化デジタル情報データを得る暗号化処理部と、

該暗号化処理部から得られる暗号化デジタル情報データと上記タイミング基準コードデータとを含んだ暗号化ワード列データを形成するデータ多重部と、

該データ多重部から得られる上記暗号化ワード列データを伝送すべく送出するデータ送出部と、

を備えて構成されるデータ伝送装置。

10. 暗号化処理部が、デジタル情報データとタイミング基準コードデータとを含んだワード列データから、デジタル情報データとタイミング基準コードデータとを分離して取り出すデータ分離部を備え、該データ分離部から得られる上記デジタル情報データに基づく暗号化デジタル情報データを得ることを特徴とする請求の範囲第9項記載のデータ伝送装置。

11. 暗号化処理部が、鍵データを送出する鍵データ送出部、及び、デジタル情報データと乱数データもしくは擬似乱数データとに禁止コードを演算出力として発生することがない演算処理を施し、該演算処理により得られる演算出力を暗号化デジタル情報データとして送出する暗号化部を含んで構成されることを特徴とする請求の範囲第9項記載のデータ伝送装置。

12. 暗号化部が、入力データに対応して鍵データ送出部から送出される鍵データに応じた規則に従って暗号データを出力する暗号形成部が出力する上記暗号データの一部を取り出すことにより乱数データもしくは擬似乱数データを得るビット取出部を含んで構成される乱数発生部を備えていることを特徴とする請求の範囲第11項記載のデータ伝送装置。

13. 暗号化部が、入力データに対応して鍵データ送出部から送出される鍵データに応じた規則に従って暗号データを出力する暗号形成部と、該暗号形成部が出力する暗号データの全部もしくは部分を上記入力データとして上記暗号形成部に戻して該暗号形成部に帰還をかけるレジスタ部と、上記暗号形成部が出力する暗号データの一部を取り出すことにより乱数データもしくは擬似乱数データを得るビット取出部とを含んで構成される乱数発生部を備えていることを特徴とする請求の範囲第11項記載のデータ伝送装置。

14. 暗号化部が、禁止コードを含まない複数の設定ワードデータが格納されたメモリ手段を備え、デジタル情報データと乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記デジタル情報データを構成する複数の情報ワードデータにより上記メモリ手段の読出アドレスを制御して、上記複数の設定ワードデータを上記複数の情報ワードデータと予め定められた対応関係を有するものとして読み出すとともに、上記乱数データもしくは擬似乱数データに応じて上記予め定められた対応関係を変化させることにより行い、暗号化デジタル情報データを上記メモリ手段からの読出出力データとして得ることを特徴とする請求の範囲第11項記載のデータ伝送装置。

15. 暗号化部が、デジタル情報データと乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記デジタル情報データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータ、及び、上記デジタル情報データがとり得る情報コードの個数をあらわすデータを用いて行う、上記デジタル情報データと上記乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算となす加減剰余演算部を備えることを特徴とする請求の範囲第11項記載のデータ伝送装置。

16. 暗号化部が、デジタル情報データについての書込み及び読出しにより、該デジタル情報データを、とり得る情報コードの範囲の一方の端部側に禁止コードが位置することになるワード位置変換ワード列データに変換するデータ変換を行うメモリ手段と、上記ワード位置変換ワード列データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータ、及び、上記ワード位置変換ワード列データがとり得る情報コードの個数をあらわすデータを用いての、上記ワード位置変換ワード列データと上記乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算を行う加減剰余演算部とを備え、上記デジタル情報データと上記乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記メモリ手段によるデータ変換と上記加減剰余演算部による加算、減算及び剰余演算となすことを特徴とする請求の範囲第11項記載のデータ伝送装置。

17. タイミング識別用コードを含む複数のコードが、情報をあらわす情報コードとしては使用されない禁止コードとされて形成されたデジタル情報データと、上記タイミング識別用コードが用いられたタイミング基準コードデータと、を含んだワード列データにおける上記デジタル情報データに、上記禁止コードを発生させない暗号化処理を施して、上記禁止コードを含まない暗号化デジタル情報データを得るとともに、該暗号化デジタル情報データと上記タイミング基準コードデータとを含んだ暗号化ワード列データを形成し、該暗号化ワード列データを伝送すべく送出し、

送出された暗号化ワード列データを得て、該暗号化ワード列データから取り出された暗号化デジタル情報データに復号化処理を施して再生デジタル情報データを得るとともに、該再生デジタル情報データと上記タイミング基準コードデータとを含んだ再生ワード列データを形成するデータ伝送方法。

18. デジタル情報データとタイミング基準コードデータとを含んだワード列データに、タイミング基準コードデータを分離するデータ分離処理を施して、デジタル情報データを得、該デジタル情報データに基づく暗号化デジタル情報データを得

るとともに、送出された暗号化ワード列データに、タイミング基準コードデータを分離するデータ分離処理を施して、暗号化デジタル情報データを得、該暗号化デジタル情報データに基づく再生デジタル情報データを得ることを特徴とする請求の範囲第17項記載のデータ伝送方法。

19. デジタル情報データと第1の乱数データもしくは擬似乱数データとに、禁止コードを演算出力として発生することがない演算処理を施し、該演算処理により得られる演算出力を取り出して暗号化デジタル情報データを得るとともに、該暗号化デジタル情報データと第2の乱数データもしくは擬似乱数データとに演算処理を施し、該演算処理により得られる演算出力を取り出して再生デジタル情報データを得ることを特徴とする請求の範囲第17項記載のデータ伝送方法。

20. 入力データに対応して鍵データに応じた規則に従って暗号データを出力する暗号形成部が出力する上記暗号データの一部を取り出すことにより、第1もしくは第2の乱数データもしくは擬似乱数データを得ることを特徴とする請求の範囲第19項記載のデータ伝送方法。

21. 入力データに対応して鍵データに応じた規則に従って暗号データを出力する暗号形成部に、上記暗号データの全部もしくは部分を入力データとして戻す帰還をかけるとともに、上記暗号形成部が出力する暗号データの一部を取り出すことにより、第1もしくは第2の乱数データもしくは擬似乱数データを得ることを特徴とする請求の範囲第19項記載のデータ伝送方法。

22. デジタル情報データと第1の乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記禁止コードを含まない複数の第1の設定ワードデータが格納された第1のメモリ手段を用意し、上記デジタル情報データを構成する複数の第1の情報ワードデータにより上記第1のメモリ手段の読出アドレスを制御して、上記複数の第1の設定ワードデータを上記複数の第1の情報ワードデータと予め定められた第1の対応関係を有するものとして読み出すとともに、上記第1の乱数データもしくは擬似乱数データに応じて上記予め定められた第1の対応関係を変化させることにより行い、暗号化デジタル情報データを上記第1のメモリ手段からの読出出力データとして得るとともに、上記暗号化デジタル情報データと第2の乱数データもしくは擬似乱数データとに施す演算処理を、上記禁止コードを含まない複数の第2の設定ワードデータが格納された第2のメモリ手段を用意し、上記暗号化デジタル情報データを構成する複数の第2の情報ワードデータにより上記第2のメモリ手段の読出アドレスを制御して、上記複数の第2の設定ワ

ードデータを上記複数の第2の情報ワードデータと予め定められた第2の対応関係を有するものとして読み出すとともに、上記第2の乱数データもしくは擬似乱数データに応じて上記第2の予め定められた対応関係を変化させることにより行い、再生デジタル情報データを上記第2のメモリ手段からの読出出力データとして得ることを特徴とする請求の範囲第19項記載のデータ伝送方法。

23. デジタル情報データと第1の乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記デジタル情報データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータ、及び、上記デジタル情報データがとり得る情報コードの個数をあらわすデータを用いて行う、上記デジタル情報データと上記第1の乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算となすとともに、暗号化デジタル情報データと第2の乱数データもしくは擬似乱数データとに施す演算処理を、上記暗号化デジタル情報データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータ、及び、上記暗号化デジタル情報データがとり得る情報コードの個数をあらわすデータを用いて行う、上記暗号化デジタル情報データと上記第2の乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算となすことを特徴とする請求の範囲第19項記載のデータ伝送方法。

24. デジタル情報データと第1の乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記デジタル情報データについての、第1のメモリ手段への書込み及び該第1のメモリ手段からの読出しによる、とり得る情報コードの範囲の一方の端部側に禁止コードが位置することになるワード位置変換ワード列データへの変換、及び、該ワード位置変換ワード列データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータと、上記ワード位置変換ワード列データがとり得る情報コードの個数をあらわすデータと、を用いて行う、上記ワード位置変換ワード列データと上記乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算、となすとともに、暗号化デジタル情報データと第2の乱数データもしくは擬似乱数データとに施す演算処理を、上記暗号化デジタル情報データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータ、及び、上記暗号化デジタル情報データがとり得る情報コードの個数をあらわすデータを用いて行う、上記暗号化デジタル情報データと上記第2の乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算、及び、該加算、減算及び剰余演算により得られる上記ワード位置変換ワード列データについての、第2のメモリ手段への書込み及び該第2のメモリ手段からの読出しによる、再生デジタル情報データへの変換、となすことを特徴とする請

求の範囲第19項記載のデータ伝送方法。

25. タイミング識別用コードを含む複数のコードが、情報をあらわす情報コードとしては使用されない禁止コードとされて形成されたデジタル情報データと、上記タイミング識別用コードが用いられたタイミング基準コードデータと、を含んだワード列データにおける上記デジタル情報データに、上記禁止コードを発生させない暗号化処理を施して、上記禁止コードを含まない暗号化デジタル情報データ得る暗号化処理部と、

該暗号化処理部から得られる暗号化デジタル情報データと上記タイミング基準コードデータとを含んだ暗号化ワード列データを形成する第1のデータ多重部と、

該第1のデータ多重部から得られる上記暗号化ワード列データを伝送すべく送出するデータ送出部と、

該データ送出部により送出された暗号化ワード列データを得て、該暗号化ワード列データから取り出された暗号化デジタル情報データに、復号化処理を施して再生デジタル情報データを得る復号化処理部と、

該復号化処理部から得られる再生デジタル情報データと上記タイミング基準コードデータとを含んだ再生ワード列データを形成する第2のデータ多重部と、を備えて構成されるデータ伝送装置。

26. 暗号化処理部が、デジタル情報データとタイミング基準コードデータとを含んだワード列データに、タイミング基準コードデータを分離するデータ分離処理を施して、デジタル情報データを得、該デジタル情報データに基づく暗号化デジタル情報データを得るとともに、復号化処理部が、暗号化ワード列データに、タイミング基準コードデータを分離するデータ分離処理を施して、暗号化デジタル情報データを得、該暗号化デジタル情報データに基づく再生デジタル情報データを形成することを特徴とする請求の範囲第25項記載のデータ伝送装置。

27. 暗号化処理が、第1の鍵データを送出する第1の鍵データ送出部、及び、デジタル情報データと第1の乱数データもしくは擬似乱数データとに、禁止コードを演算出力として発生することがない演算処理を施し、該演算処理により得られる演算出力を取り出して暗号化デジタル情報データとして送出する暗号化部を含んで構成されるとともに、復号化処理部が、第2の鍵データを送出する第2の鍵データ送出部、及び、上記暗号化デジタル情報データと第2の乱数データもしくは擬似乱数データとに演算処理を施し、該演算処理により得られる演算出力を取り出して再生デジタル情報データを得る復号化部を含んで構成されることを特徴とする請求の範囲第25項記載のデータ伝送装置。

28. 暗号化部が、入力データに対応して第1の鍵データに応じた規則に従って第1の暗号データを出力する第1の暗号形成部が出力する上記第1の暗号データの一部を取り出すことにより、第1の乱数データもしくは擬似乱数データを得、また、復号化部が、入力データに対応して第2の鍵データに応じた規則に従って第2の暗号データを出力する第2の暗号形成部が出力する上記第2の暗号データの一部を取り出すことにより、第2の乱数データもしくは擬似乱数データを得ることを特徴とする請求の範囲第27項記載のデータ伝送装置。

29. 暗号化部が、入力データに対応して第1の鍵データに応じた規則に従って第1の暗号データを出力する第1の暗号形成部に、上記第1の暗号データの全部もしくは部分を入力データとして戻す帰還をかけるとともに、上記第1の暗号形成部が出力する第1の暗号データの一部を取り出すことにより、第1の乱数データもしくは擬似乱数データを得、また、復号化部が、入力データに対応して第2の鍵データに応じた規則に従って第2の暗号データを出力する第2の暗号形成部に、上記第2の暗号データの全部もしくは部分を入力データとして戻す帰還をかけるとともに、上記第2の暗号形成部が出力する第2の暗号データの一部を取り出すことにより、第2の乱数データもしくは擬似乱数データを得ることを特徴とする請求の範囲第27項記載のデータ伝送装置。

30. 暗号化部が、禁止コードを含まない複数の第1の設定ワードデータが格納された第1のメモリ手段を備え、デジタル情報データと第1の乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記デジタル情報データを構成する複数の第1の情報ワードデータにより上記第1のメモリ手段の読出アドレスを制御して、上記複数の第1の設定ワードデータを上記複数の第1の情報ワードデータと予め定められた第1の対応関係を有するものとして読み出すとともに、上記第1の乱数データもしくは擬似乱数データに応じて上記予め定められた第1の対応関係を変化させることにより行い、暗号化デジタル情報データを上記第1のメモリ手段からの読出出力データとして得るとともに、復号化部が、禁止コードを含まない複数の第2の設定ワードデータが格納された第2のメモリ手段を備え、上記暗号化デジタル情報データと第2の乱数データもしくは擬似乱数データとに施す演算処理を、上記暗号化デジタル情報データを構成する複数の第2の情報ワードデータにより上記第2のメモリ手段の読出アドレスを制御して、上記複数の第2の設定ワードデータを上記複数の第2の情報ワードデータと予め定められた第2の対応関係を有するものとして読み出すとともに、上記第2の乱数データもしくは擬似乱数データに応じて上記第2の予め定められた対応関係を変化させることにより行

い、上記再生デジタル情報データを上記第2のメモリ手段からの読出出力データとして得ることを特徴とする請求の範囲第27項記載のデータ伝送装置。

31. 暗号化部が、デジタル情報データと第1の乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記デジタル情報データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータ、及び、上記デジタル情報データがとり得る情報コードの個数をあらわすデータを用いて行う、上記デジタル情報データと上記第1の乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算となす第1の加減剰余演算部を備えるとともに、復号化部が、暗号化デジタル情報データと第2の乱数データもしくは擬似乱数データとに施す演算処理を、上記暗号化デジタル情報データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータ、及び、上記暗号化デジタル情報データがとり得る情報コードの個数をあらわすデータを用いて行う、上記暗号化デジタル情報データと上記第2の乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算となす第2の加減剰余演算部を備えることを特徴とする請求の範囲第27項記載のデータ伝送装置。

32. 暗号化部が、デジタル情報データについての書込み及び読出しにより、該デジタル情報データを、とり得る情報コードの範囲の一方の端部側に禁止コードが位置にすることになるワード位置変換ワード列データに変換するデータ変換を行う第1のメモリ手段と、上記ワード位置変換ワード列データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータ、及び、上記ワード位置変換ワード列データがとり得る情報コードの個数をあらわすデータを用いての、上記ワード位置変換ワード列データと上記第1の乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算を行う第1の加減剰余演算部とを備え、上記デジタル情報データと第1の乱数データもしくは擬似乱数データとに施す、禁止コードを演算出力として発生することがない演算処理を、上記第1のメモリ手段によるデータ変換、及び、上記第1の加減剰余演算部による加算、減算及び剰余演算となすとともに、復号化部が、上記暗号化デジタル情報データがとり得る情報コードの範囲の一方の端部側における禁止コードの個数をあらわすデータ、及び、上記暗号化デジタル情報データがとり得る情報コードの個数をあらわすデータを用いての、上記暗号化デジタル情報データと上記第2の乱数データもしくは擬似乱数データとについての加算、減算及び剰余演算を行う第2の加減剰余演算部と、該第2の加減剰余演算部により行われる加算、減算及び剰余演算により得られる上記ワード位置変換ワード列データについての書込み及び読出しにより、該ワード位置変換ワード列データを再生デジタル情報データに変換するデータ変換を行う第2のメモリ手段とを備え、上記暗号化デ

ィジタル情報データと第2の乱数データもしくは擬似乱数データとに施す演算処理を、上記第2の加減余剰演算部による加算、減算及び剰余演算、及び、上記第2のメモリ手段によるデータ変換となすことを特徴とする請求の範囲第27項記載のデータ伝送装置。

図1

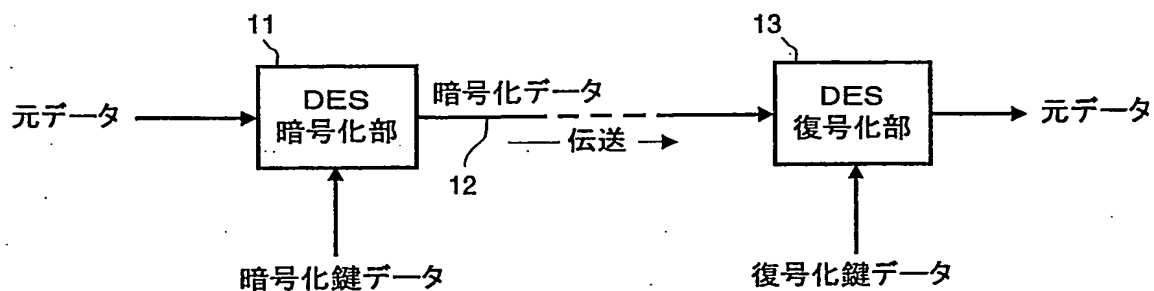


図3

HD信号(10ビットワード)についての禁止コード

000h	0000000000	3FCh	1111111100
↓	0000000001	↓	1111111101
↓	0000000010	↓	1111111110
003h	0000000011	3FFh	1111111111

図5

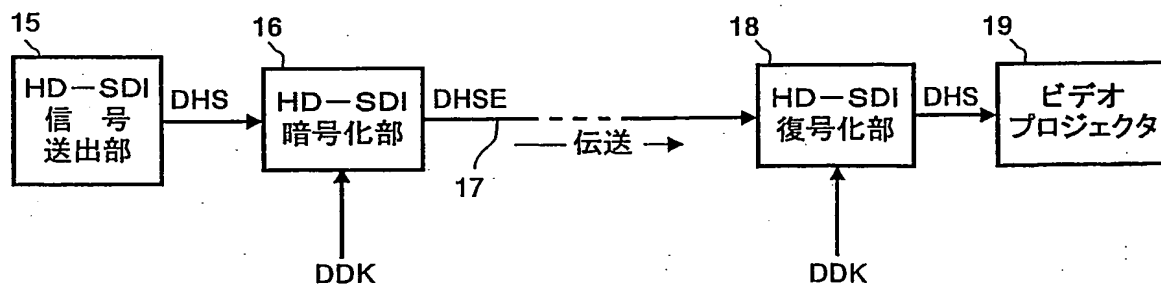
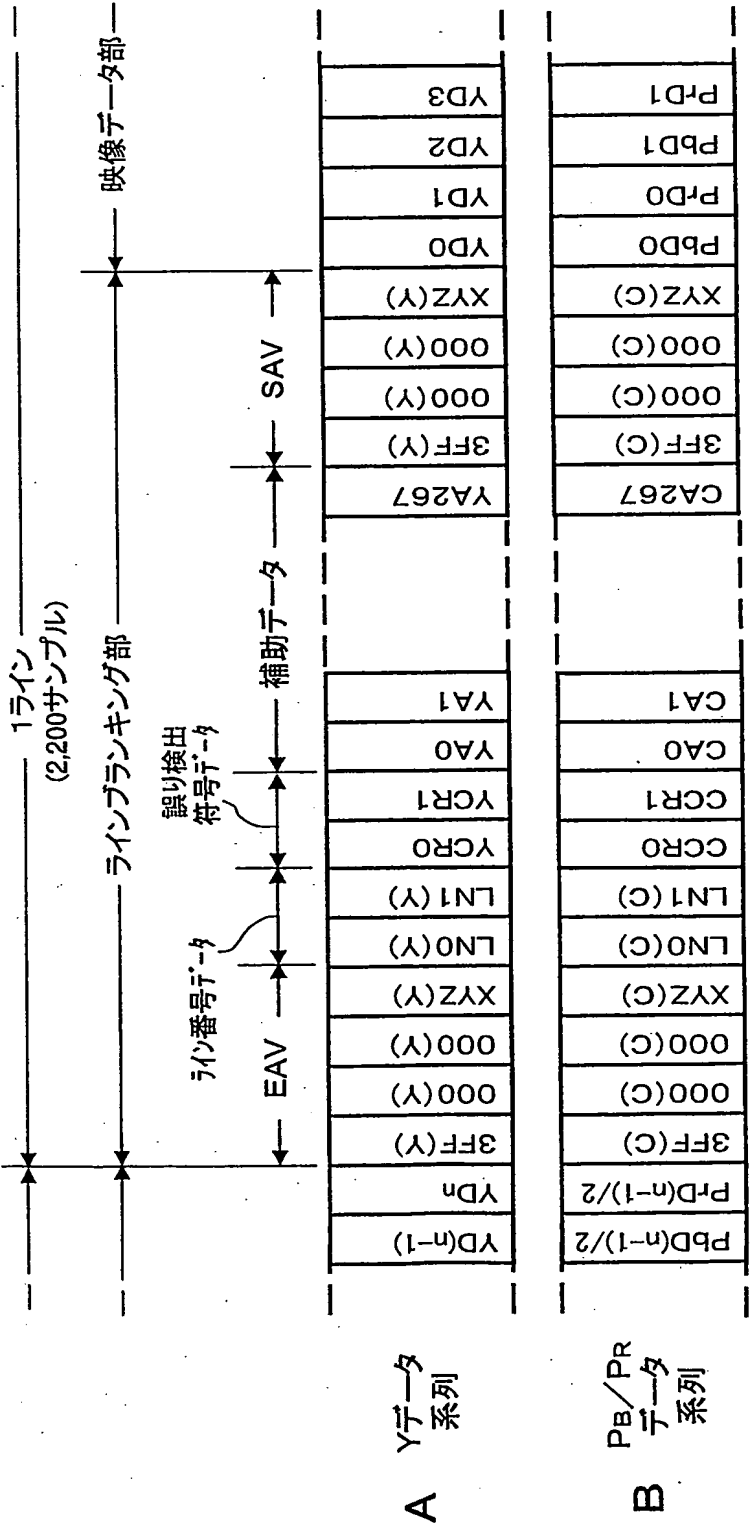


図2



YD0~YDn : Y信号データワード
PbD0~PbD(n-1)/2 : PB信号データワード
PrD0~PrD(n-1)/2 : PR信号データワード

图4

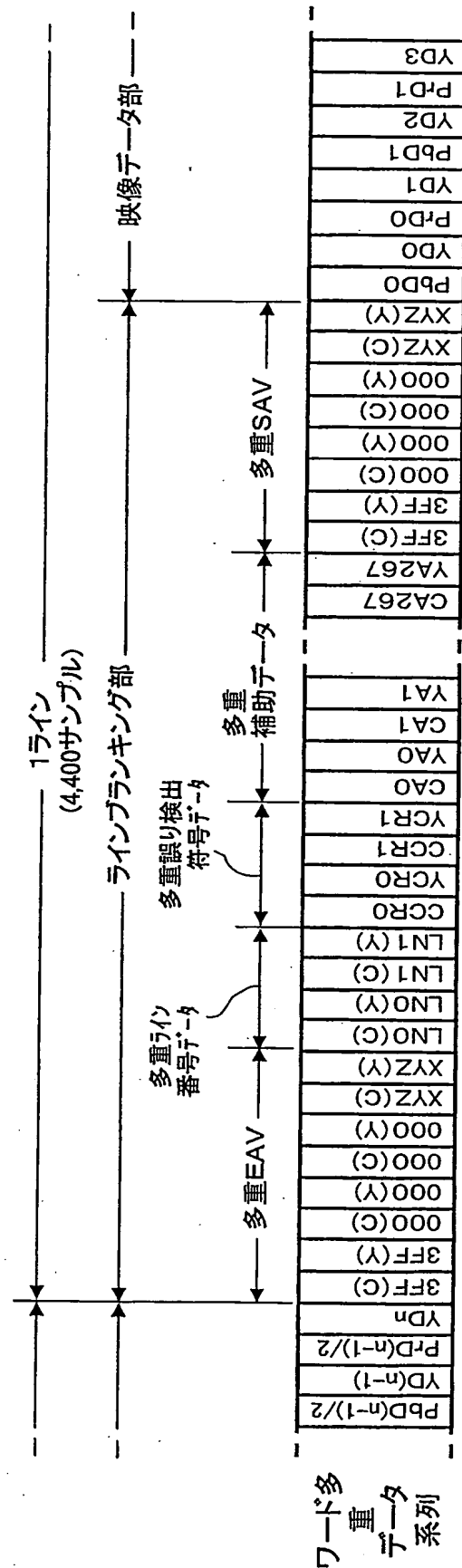


図6

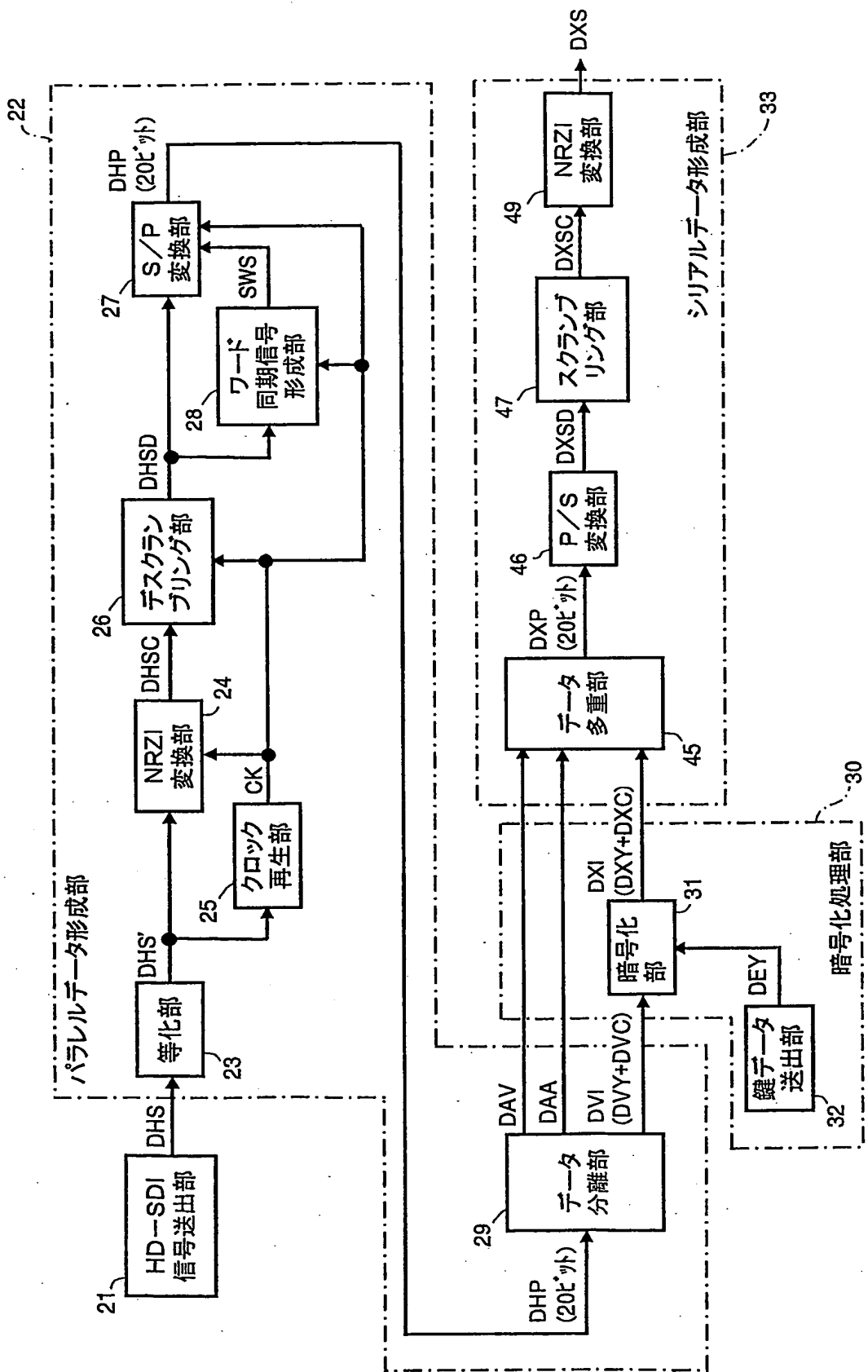


図7

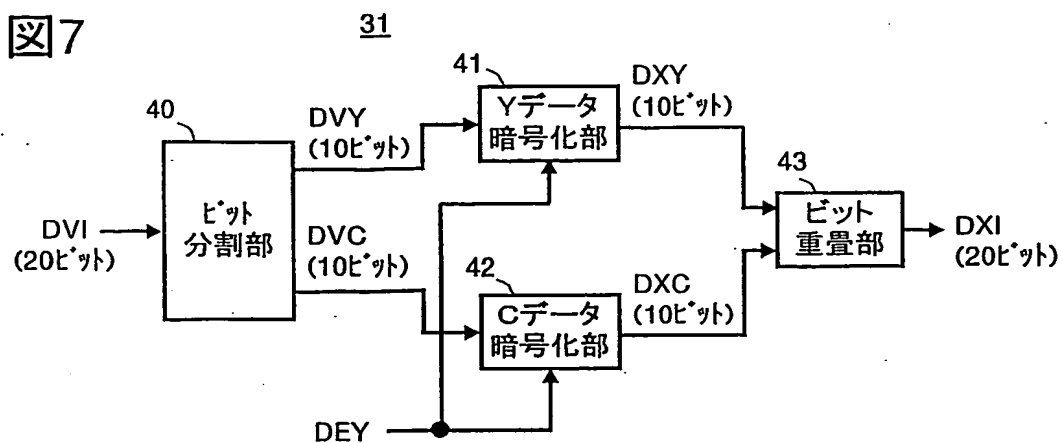


図8

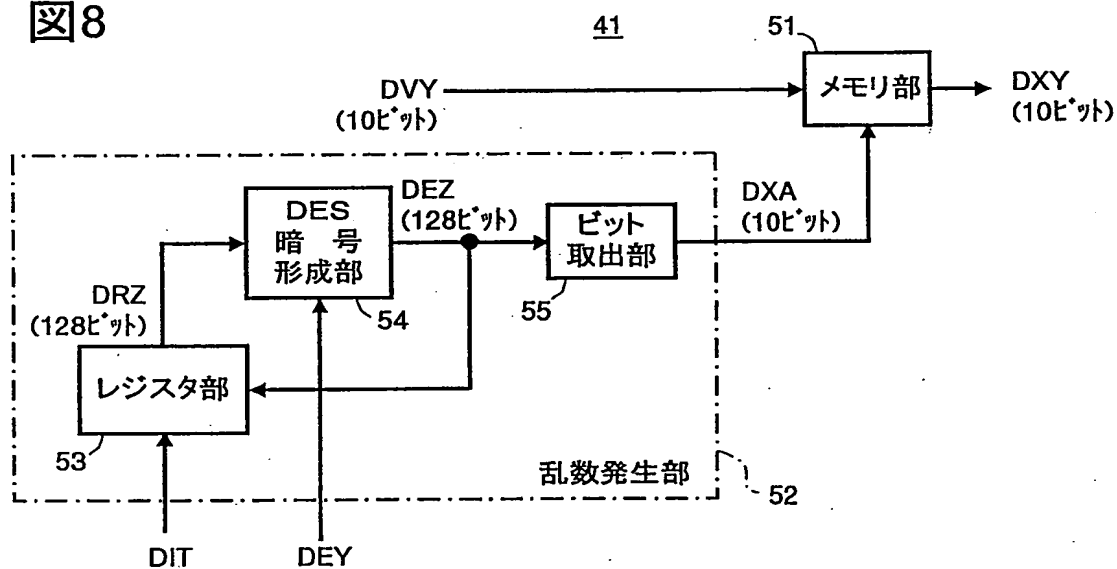


図9

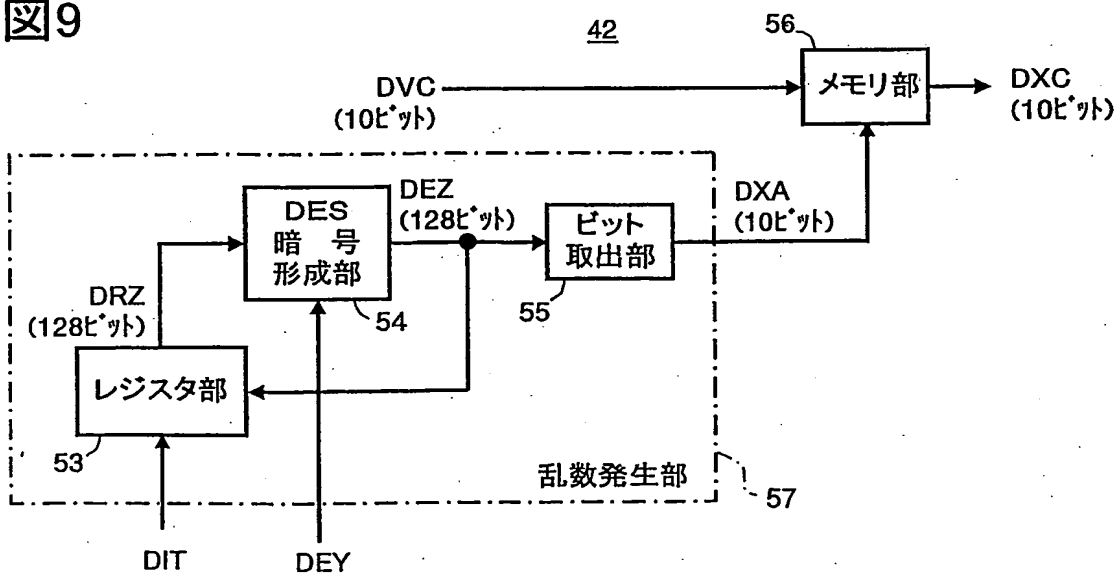


図10

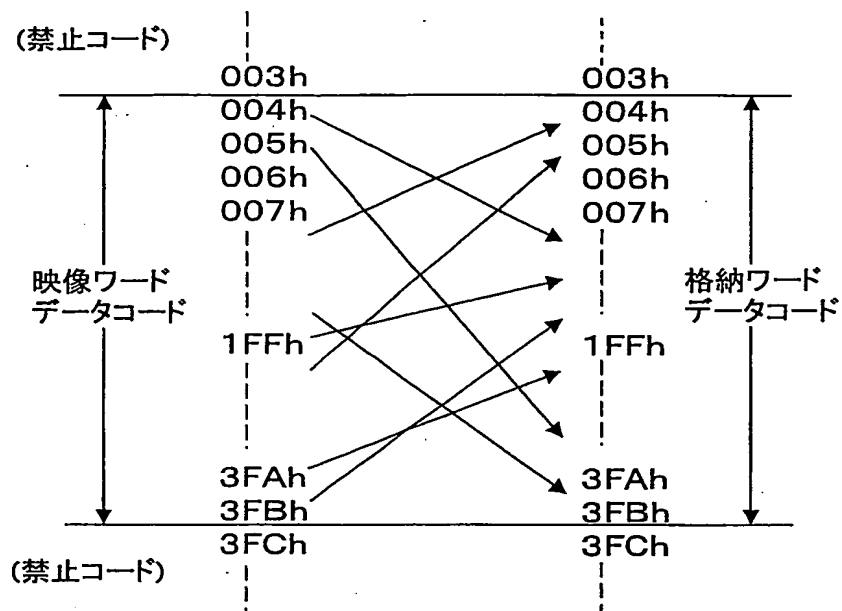


図11

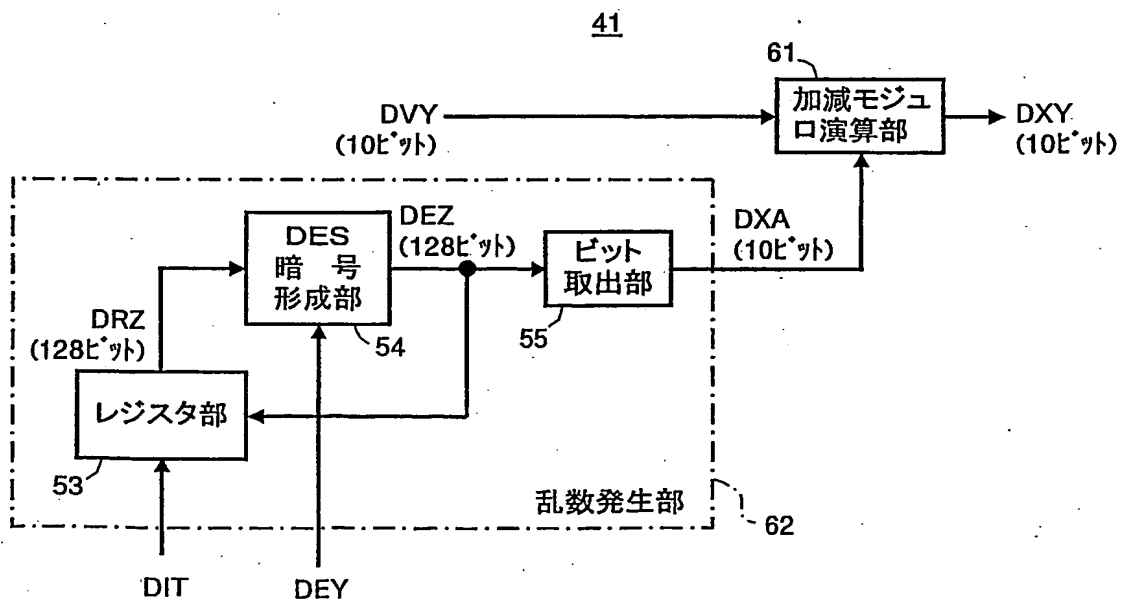


図12

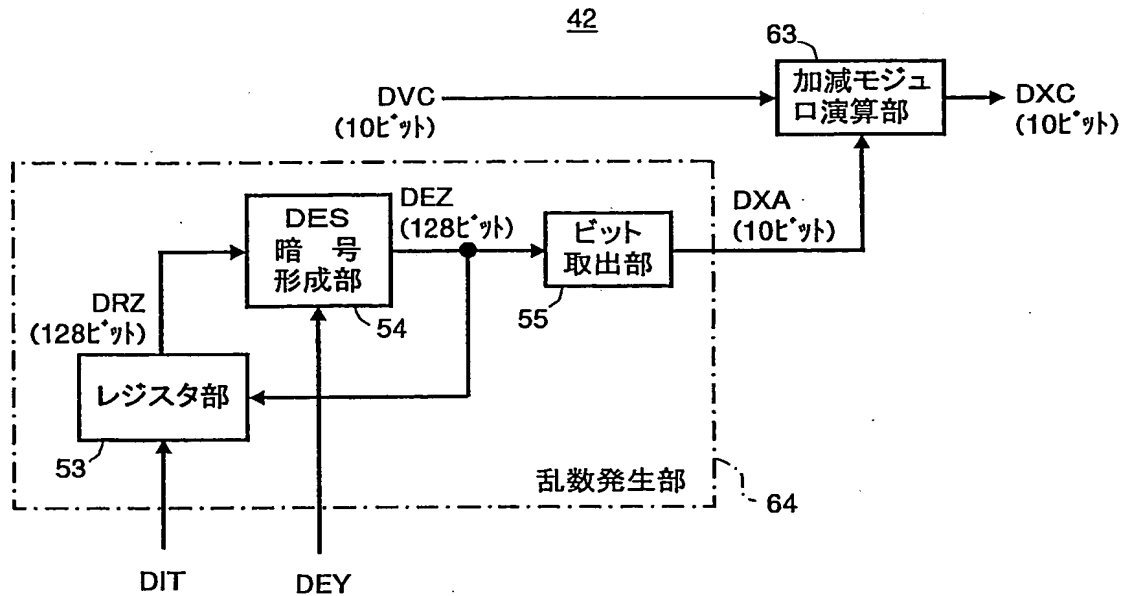


図13

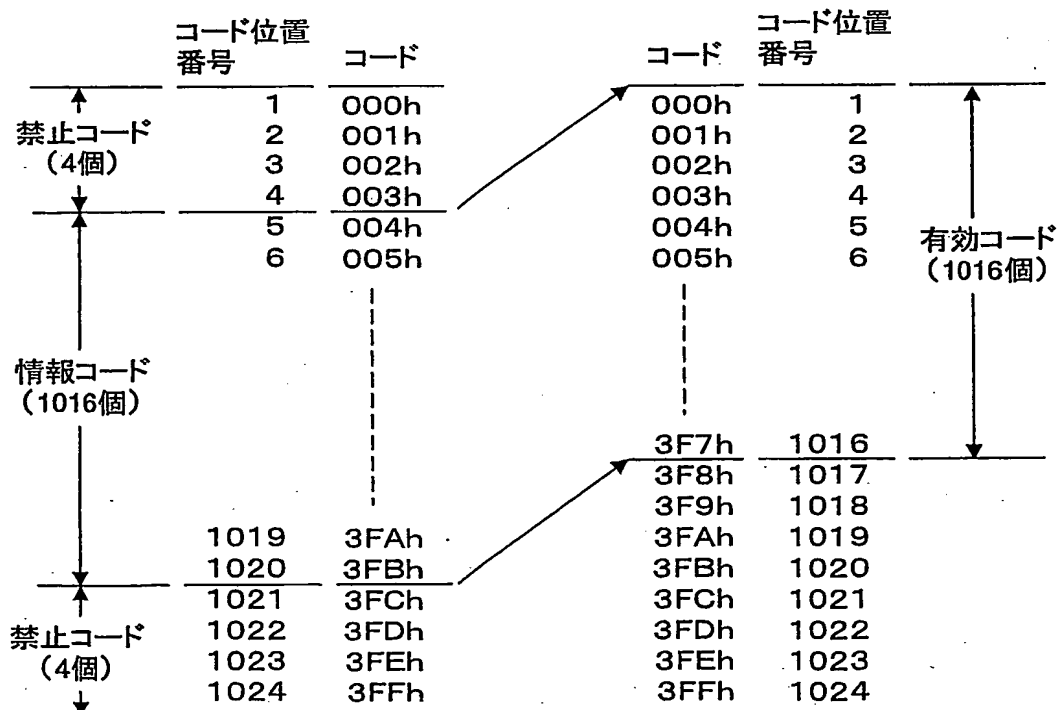


図14

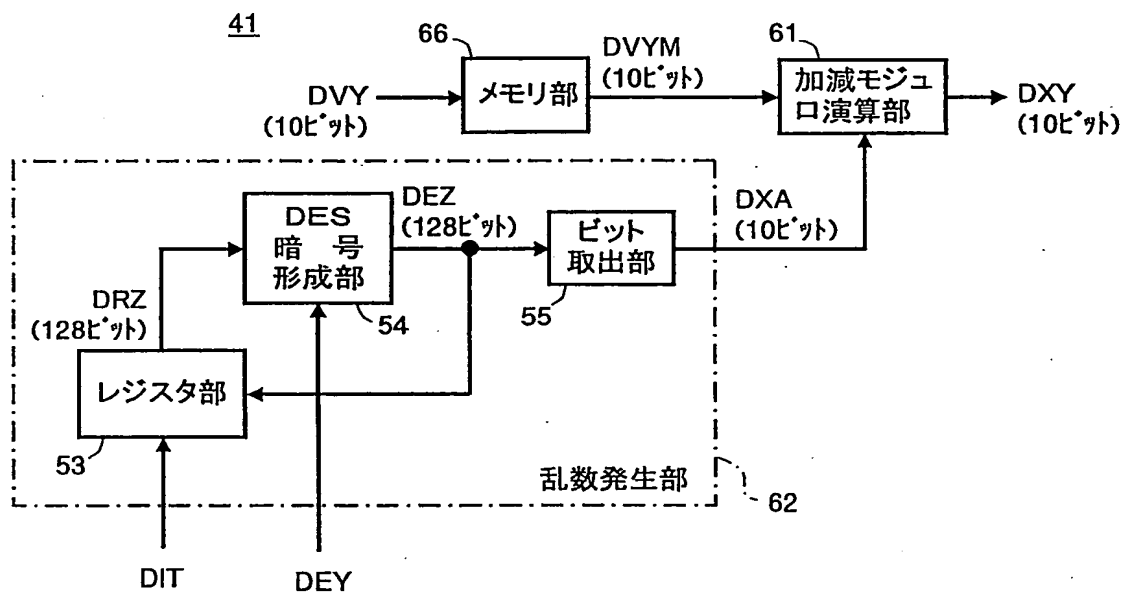


図15

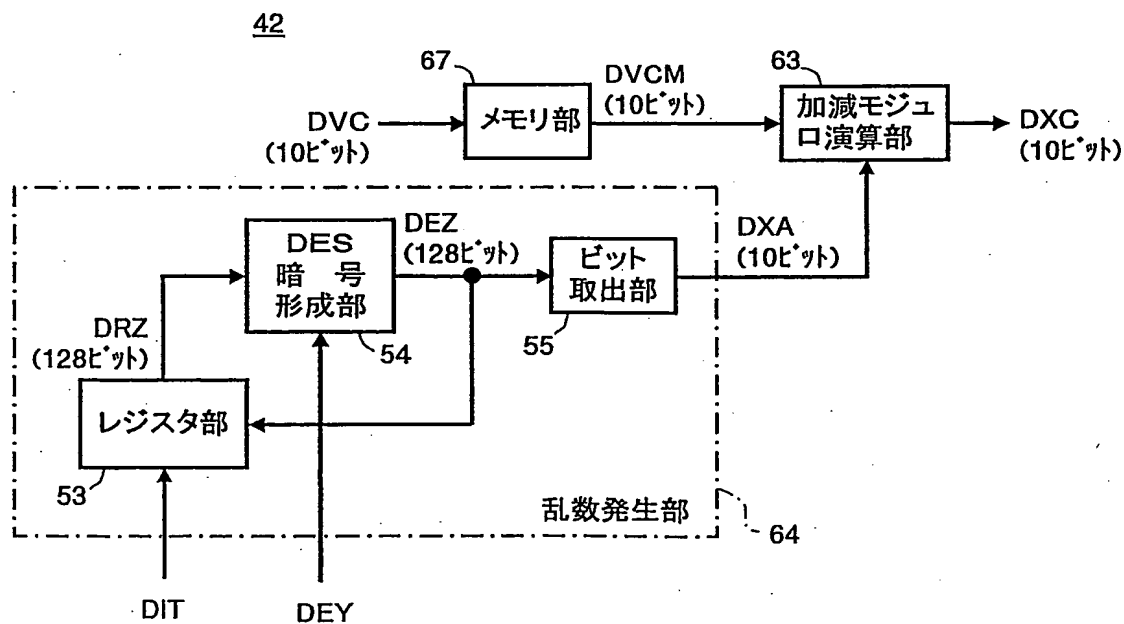


図16

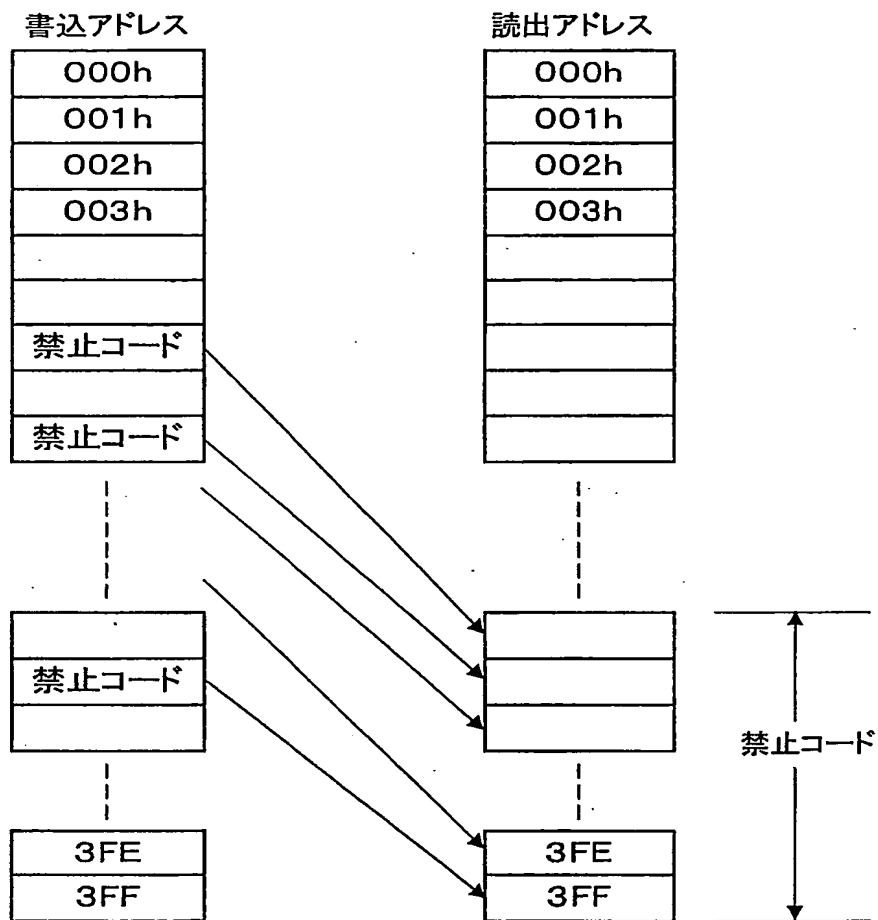


図17

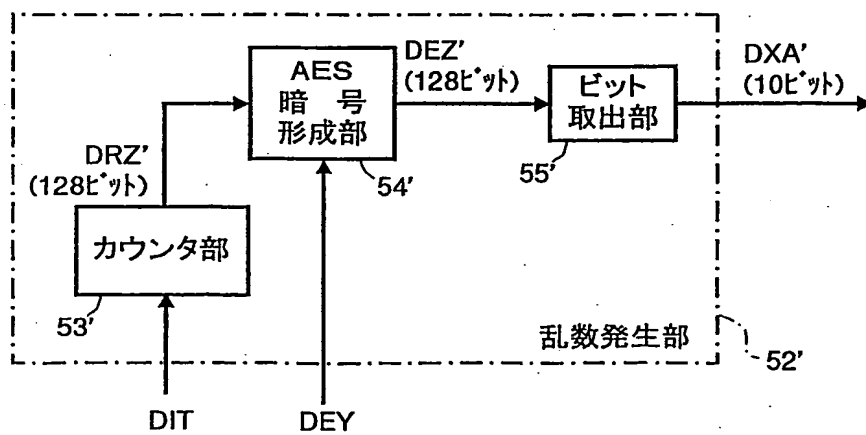


図18

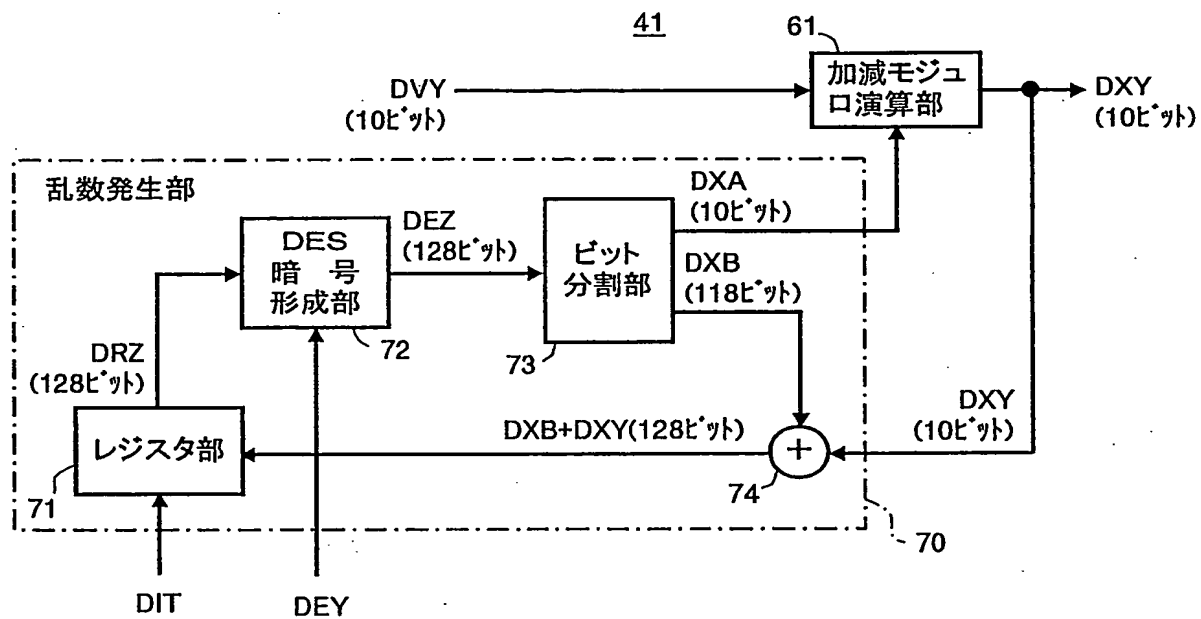


図19

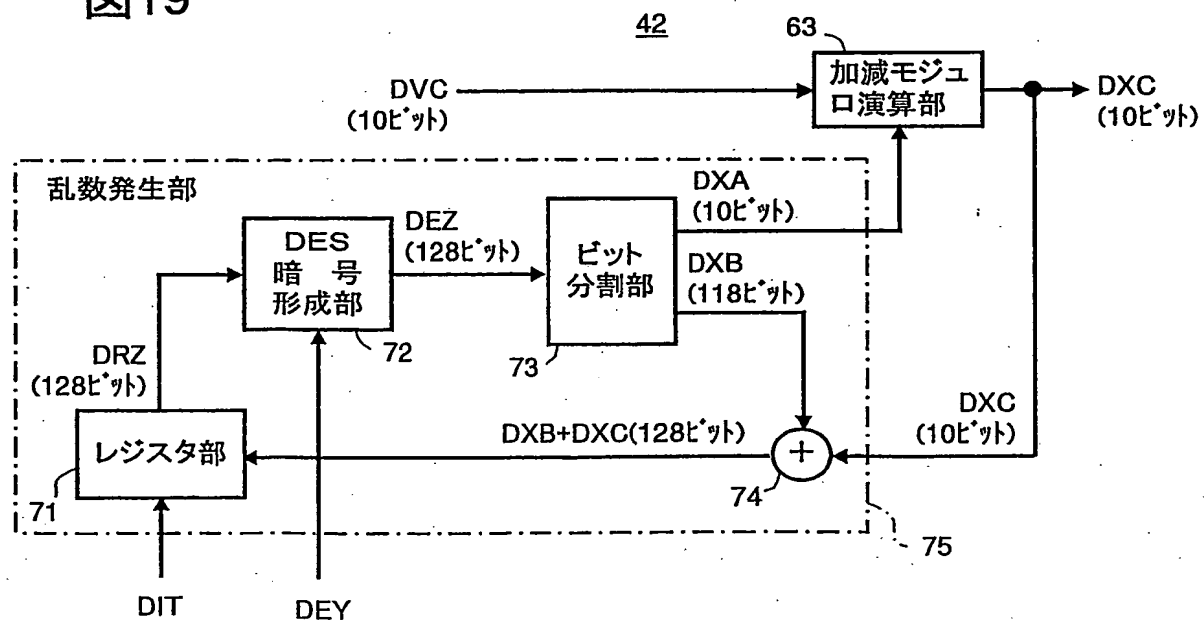


図20

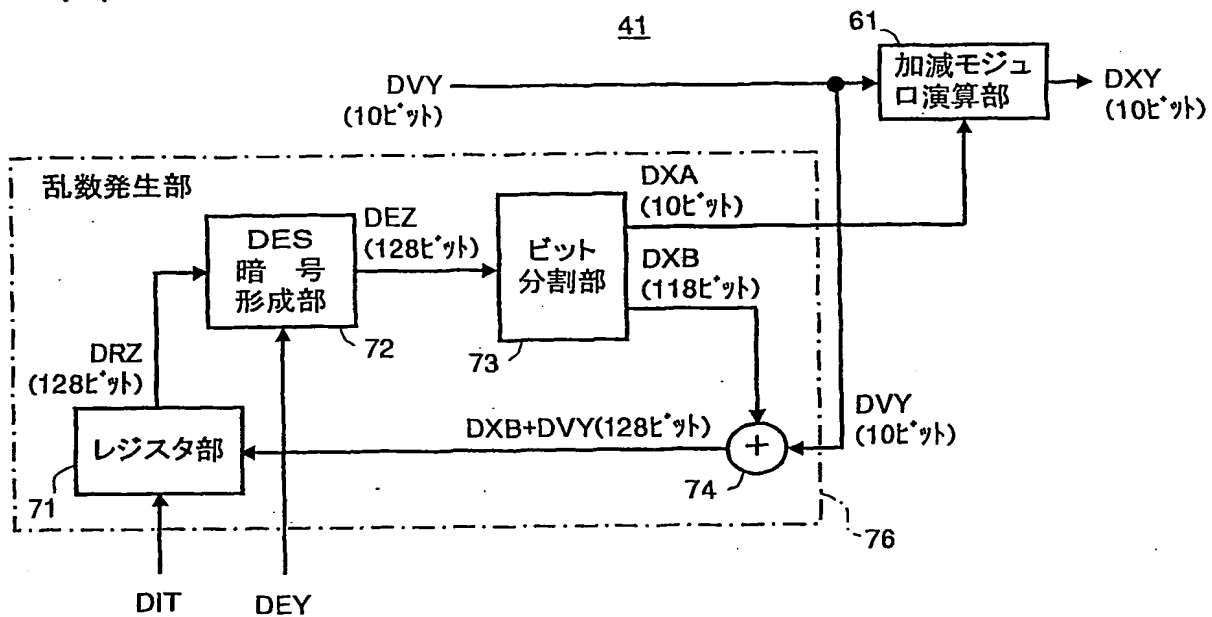


図21

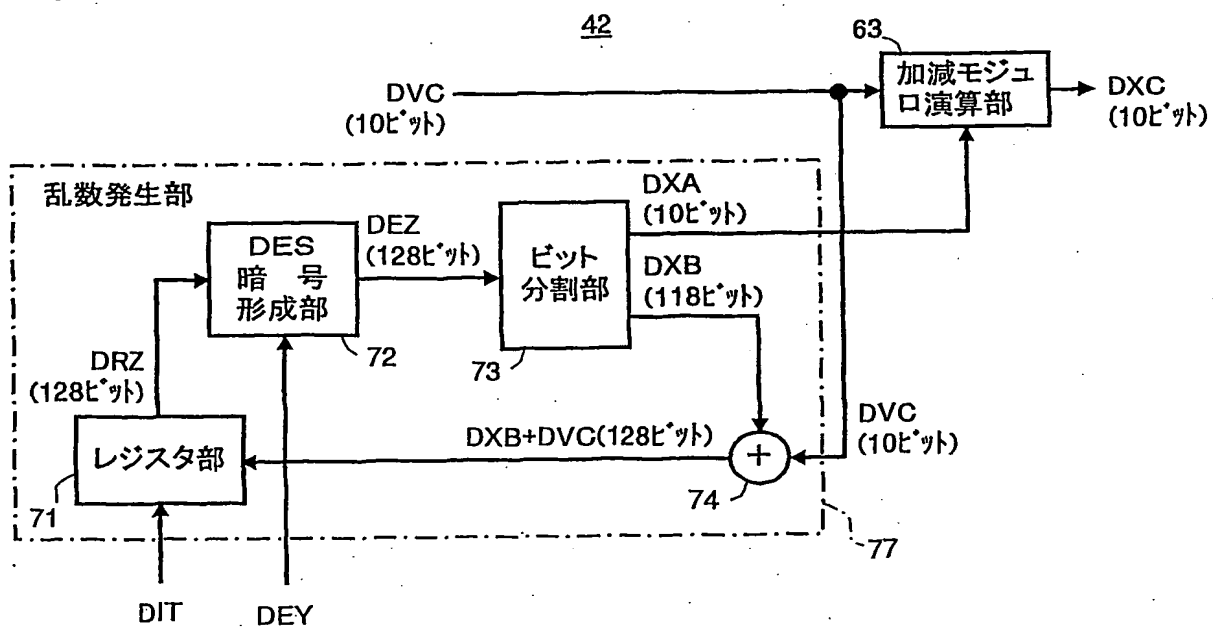


図22

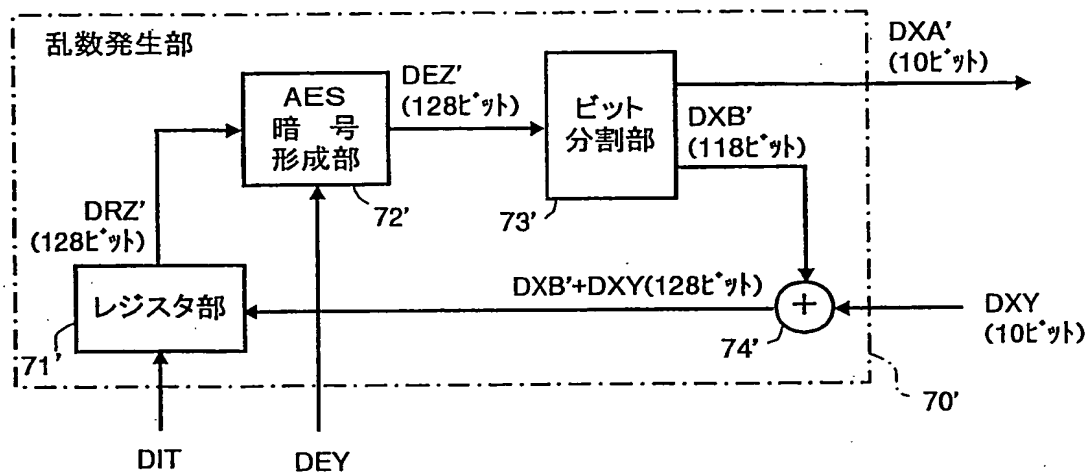


図24

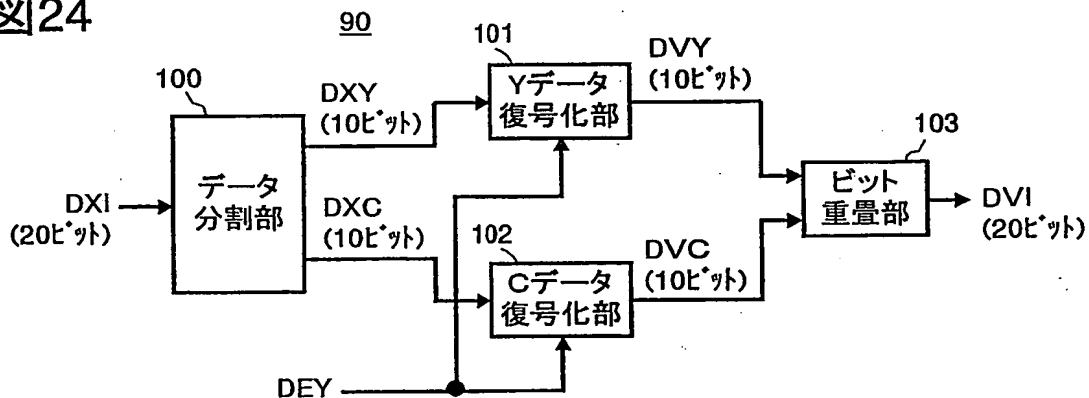


図25

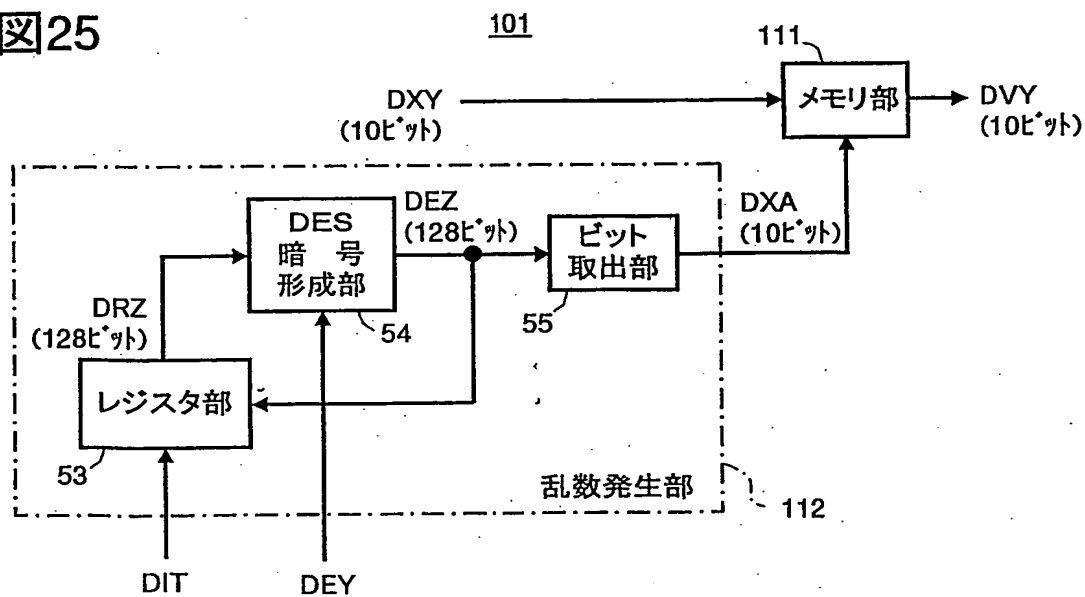
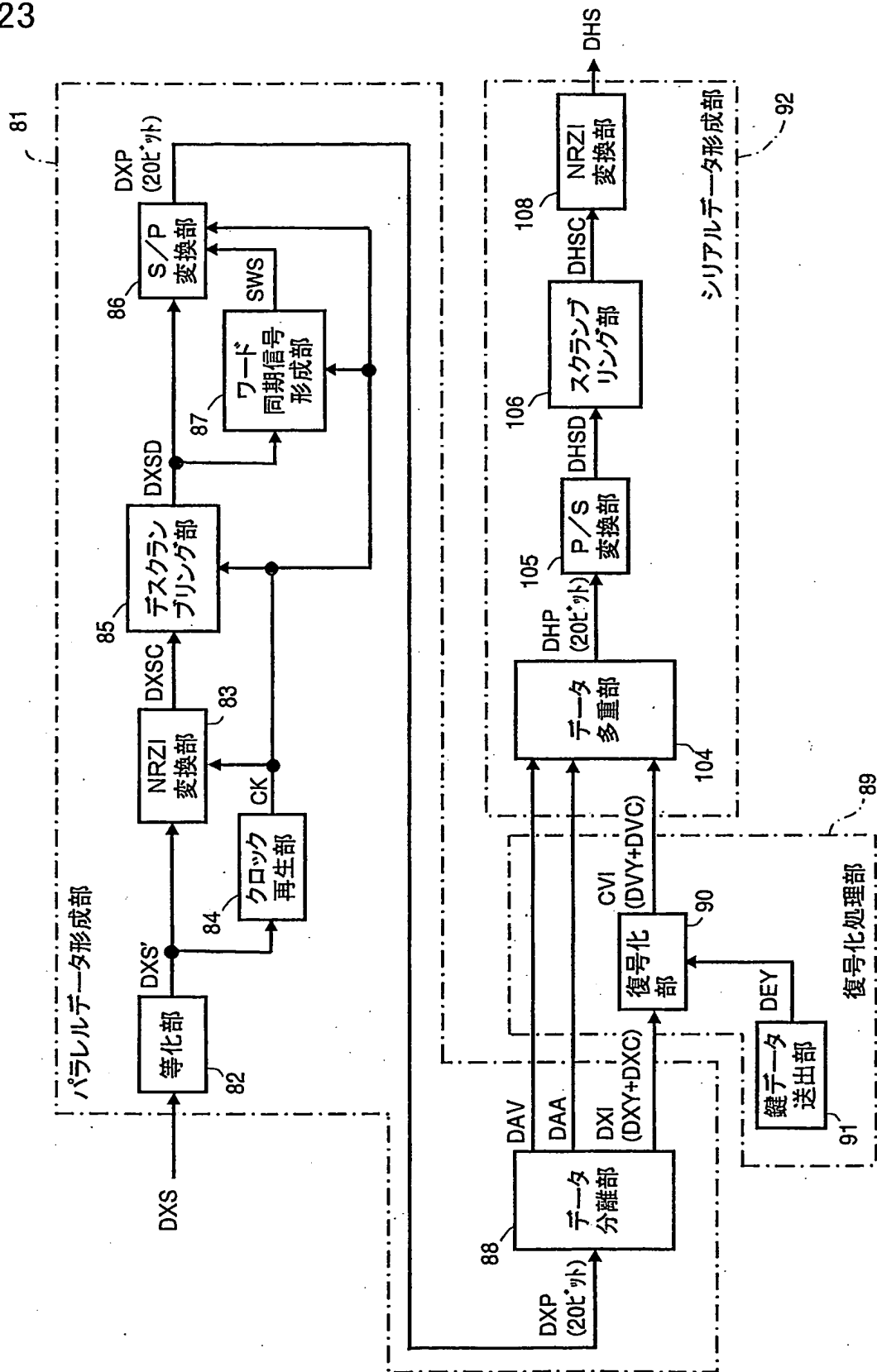


図23



14/18

図26

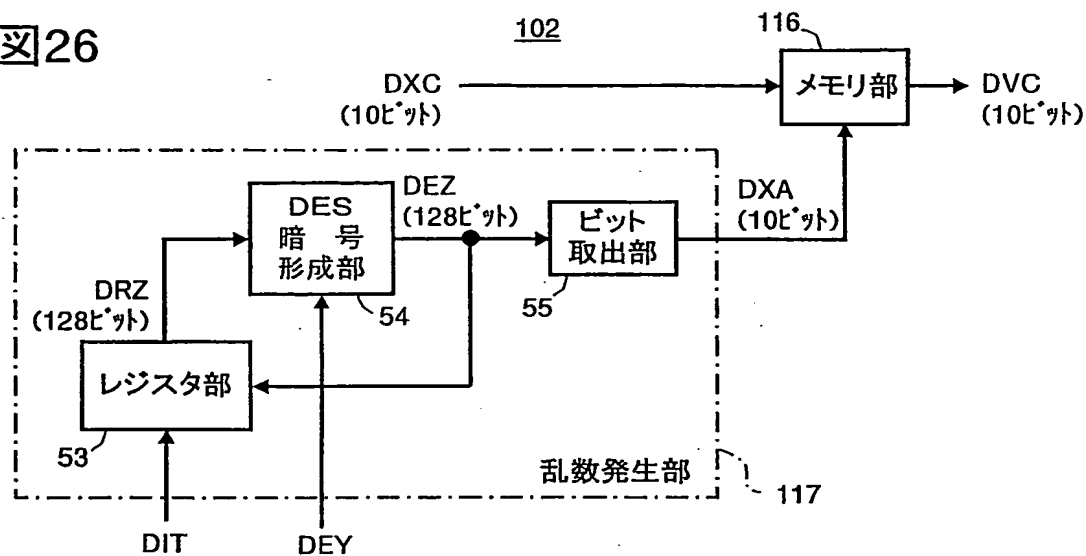


図27

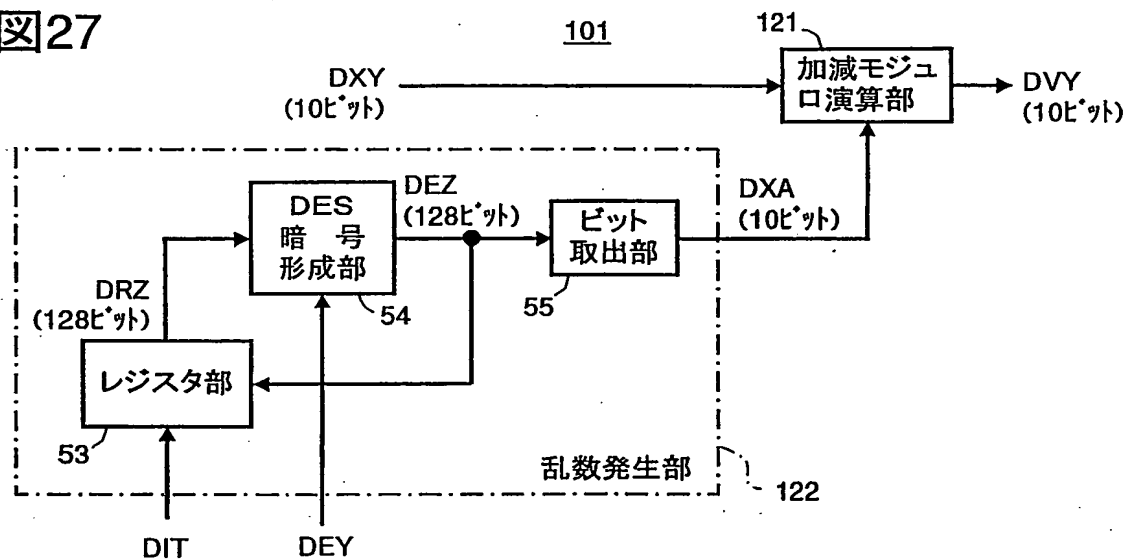


図28

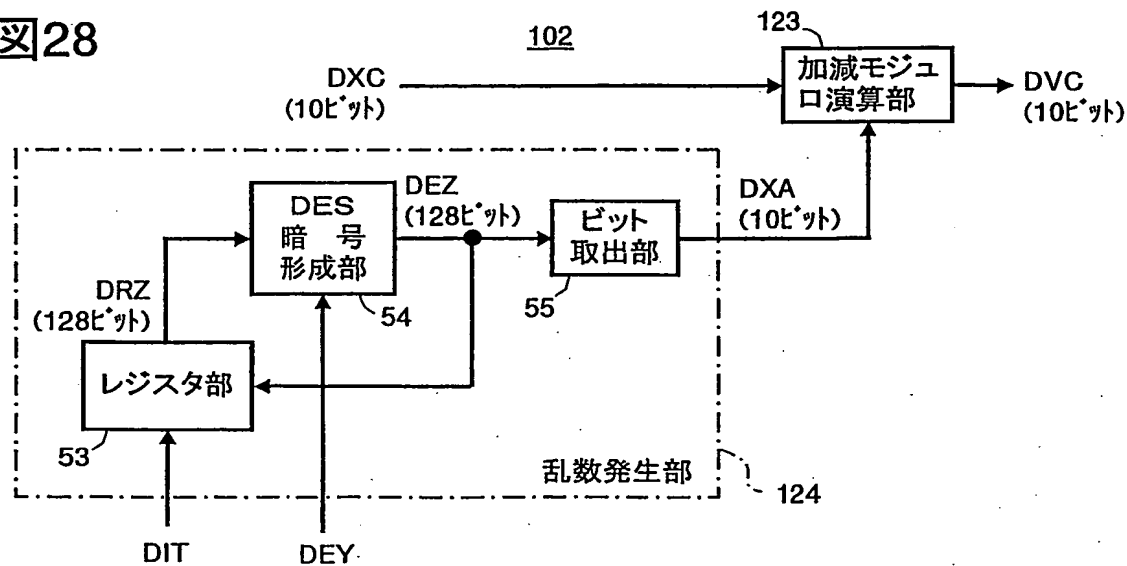


図29

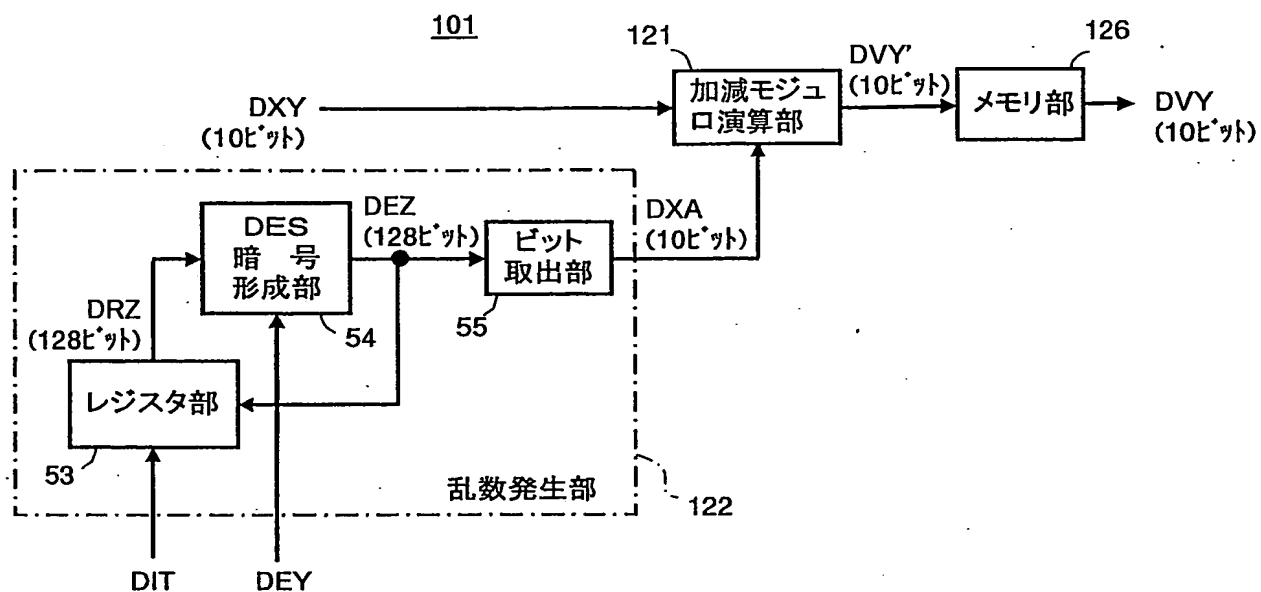


図30

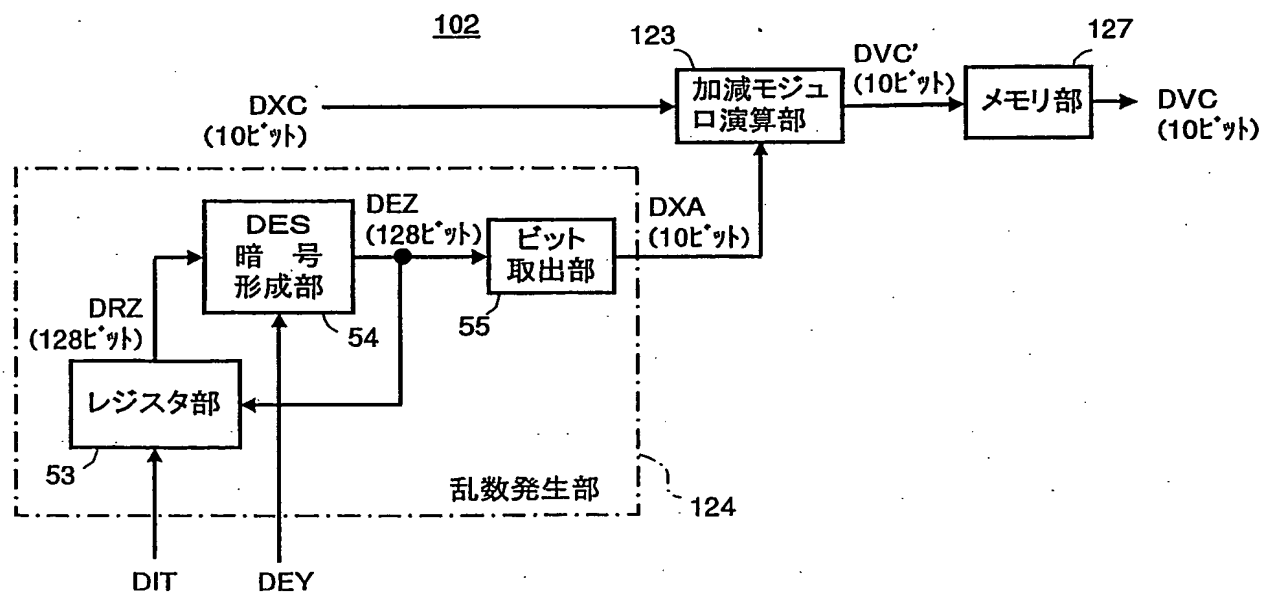


図31

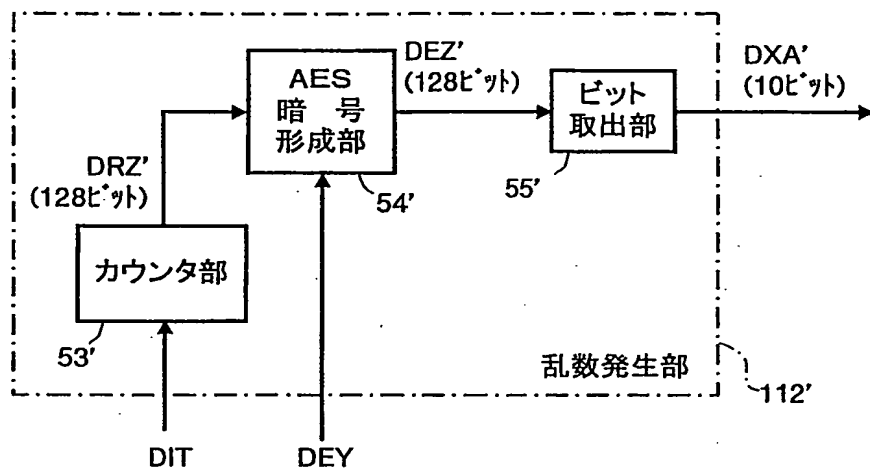


図32

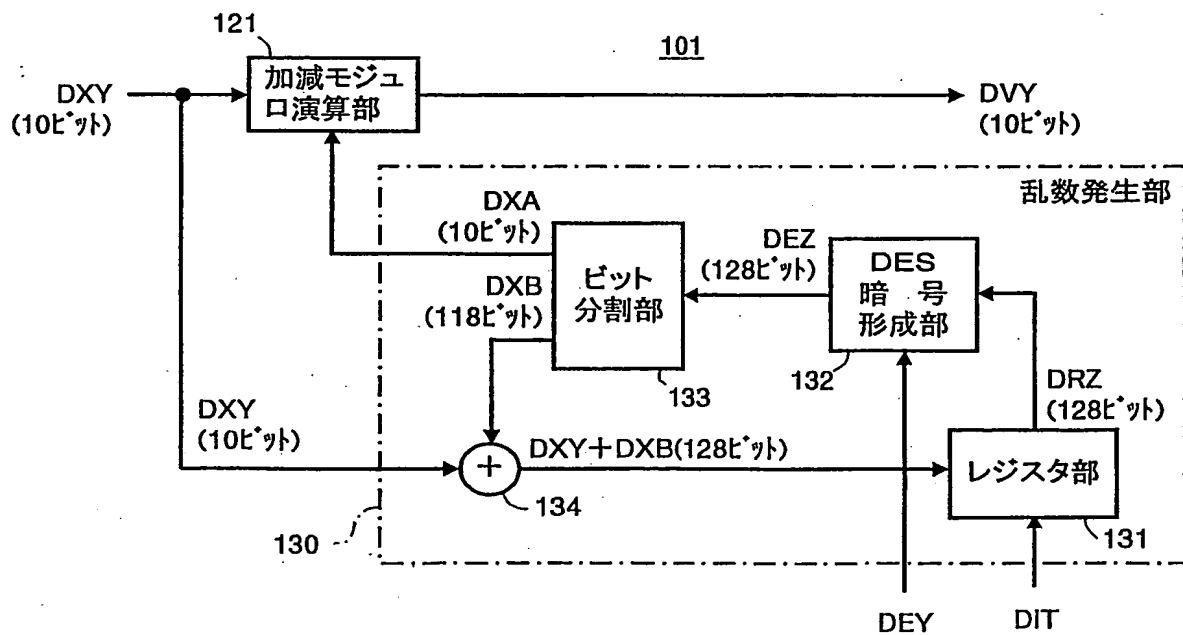


图 33

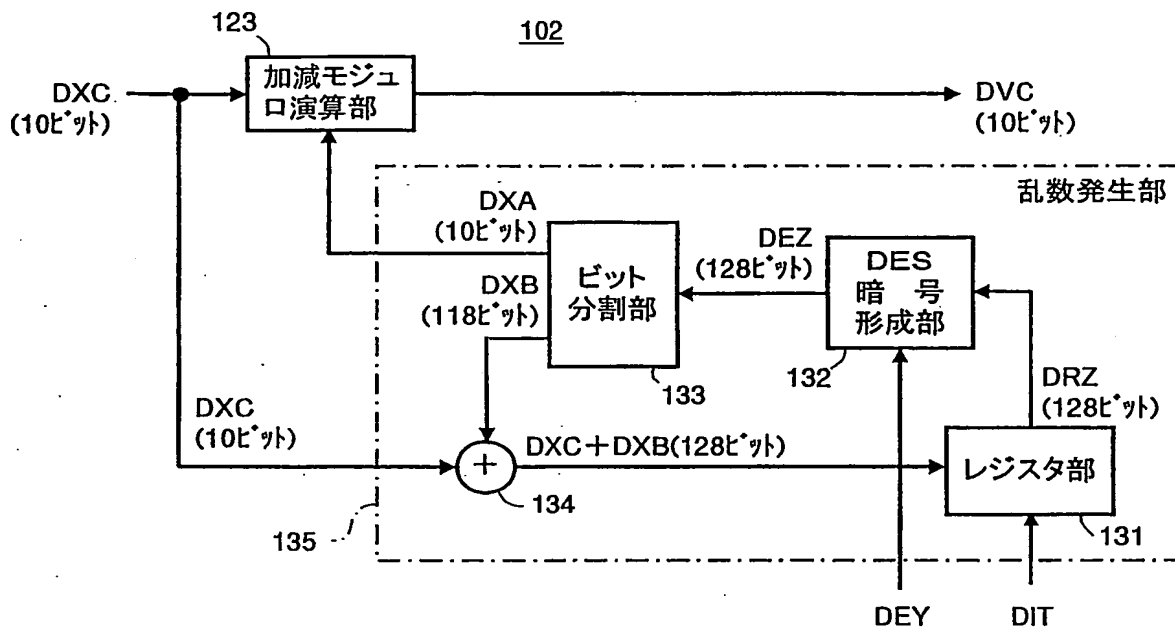
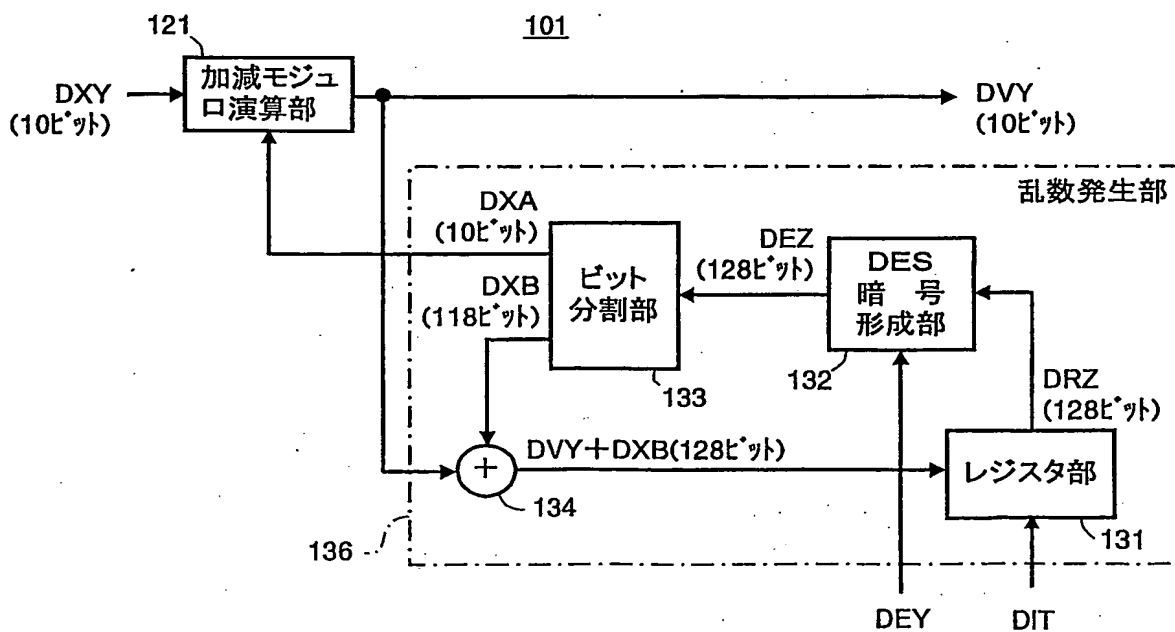


图34



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/05676

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.⁷ H04L9/08, H04L9/14, H04N11/00, H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ H04L9/08, H04L9/14, H04N11/00, H04N7/167

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 7-67140 A (Sony Corp.), 10 March, 1995 (10.03.95), Full text; Figs. 1 to 6 (Family: none)	1-32
Y	JP 63-502393 A (WEISS, Jeffrey, A.), 08 September, 1988 (08.09.88), Page 7, upper right column, line 6 to lower right column, line 21; Fig. 1 & AU 6470186 A & US 4654480 A & WO 87/003442 A & EP 248028 A & US 4754482 A & CA 1268258 A	1-32
Y	JP 10-108217 A (NEC Corp.), 24 April, 1998 (24.04.98), Full text; Figs. 1 to 3 (Family: none)	9-21, 25-32

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
16 July, 2003 (16.07.03)

Date of mailing of the international search report
29 July, 2003 (29.07.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/05676

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2001-326616 A (Sony Corp.), 22 November, 2001 (22.11.01), Full text; Figs. 1 to 19 (Family: none)	1-32
A	JP 6-225258 A (Matsushita Electric Industrial Co., Ltd.), 12 August, 1994 (12.08.94), Par. Nos. [0028] to [0029] (Family: none)	1-32
A	JP 4-179344 A (Hitachi Denshi, Ltd.), 26 June, 1992 (26.06.92); Full text; Figs. 1 to 8 (Family: none)	1-32

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁷ H04L9/08 H04L9/14 H04N11/00 H04N7/167

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁷ H04L9/08 H04L9/14 H04N11/00 H04N7/167

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2003年
日本国登録実用新案公報	1994-2003年
日本国実用新案登録公報	1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 7-67140 A (ソニー株式会社) 1995.03.10 全文, 図1-6 (ファミリーなし)	1-32

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

16.07.03

国際調査報告の発送日

29.07.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5M

4229

電話番号 03-3581-1101 内線 3597

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 63-502393 A (ウェイス, ジェフリー・エイ) 1988. 09. 08 第7頁右上欄第6行一同頁右下欄第21行, 図1 & AU 6470186 A & US 4654480 A & WO 87/003442 A & EP 248028 A & US 4754482 A & CA 1268258 A	1-32
Y	JP 10-108217 A (日本電気株式会社) 1998. 04. 24 全文, 図1-3 (ファミリーなし)	9-21, 25-32
A	JP 2001-326616 A (ソニー株式会社) 2001. 11. 22 全文, 図1-19 (ファミリーなし)	1-32
A	JP 6-225258 A (松下電器産業株式会社) 1994. 08. 12 第【0028】-【0029】段落 (ファミリーなし)	1-32
A	JP 4-179344 A (日立電子株式会社) 1992. 06. 26 全文, 図1-8 (ファミリーなし)	1-32